

---

# FEW GATES BUT MANY ZEROS

BERND BORCHERT<sup>1</sup> AND PIERRE MCKENZIE<sup>2</sup> AND KLAUS REINHARDT<sup>1</sup>

<sup>1</sup> Universität Tübingen, Sand 13, 72076 Tübingen, Germany  
*E-mail address:* `\{borchert,reinhard\}@informatik.uni-tuebingen.de`

<sup>2</sup> Informatique et recherche opérationnelle, Université de Montréal,, C.P. 6128, Succ. Centre-Ville, Montréal (Québec), H3C 3J7 Canada.  
*E-mail address:* `mckenzie@iro.umontreal.ca`

---

**ABSTRACT.** Motivated by the integer factoring problem, we define a  $d$ -gem as a  $\{+, -, \times\}$ -circuit having at most  $\ell_d$  product gates and computing, from  $\{x\} \cup \mathbb{Z}$ , a degree  $d$  polynomial having  $d$  distinct roots in  $\mathbb{Z}$ , where  $\ell_d$  is the minimum length of an addition chain for  $d$ . For  $n \leq 4$  we exhibit  $2^n$ -gems having the additional property of being skew, that is, one input to each  $\{+, -\}$ -gate is from  $\mathbb{Z}$ . We prove that such skew circuits require  $n$   $\{+, -\}$ -gates and we conclude that our  $2^n$ -gems for  $n \leq 4$  are both  $\{\times\}$ -optimal as gems and  $\{\times, +, -\}$ -optimal as skew gems. We relate our constructions to the conjectures of Blum-Cucker-Shub-Smale and of Bürgisser and we raise the unlikely possibility that  $d$ -gems might exist for every  $d$ . We exhibit  $\{\times\}$ -optimal  $d$ -gems for several values of  $d$  up to 55. We observe however that the existence of skew  $2^n$ -gems for  $n \geq 5$  would provide new solutions to the Prouhet-Tarry-Escott problem in number theory. By contrast,  $d$ -gems over the real numbers are shown to exist for every  $d$ .

## Introduction

Blum, Cucker, Shub and Smale [BCSS97] conjectured that for some  $\beta$ , any polynomial  $f(x) \in \mathbb{Z}[x]$  has at most  $(\tau(f) + 1)^\beta$  distinct roots in  $\mathbb{Z}$ , where  $\tau(f)$  is the size of a smallest  $\{+, -, \times\}$ -circuit computing  $f(x)$  from  $x$  and the constant 1. Known as the  $\tau$ -conjecture, this was the strengthening of an earlier conjecture shown by Lipton to imply that the integer factoring problem would be “too easy” to support cryptography [Li94].

Polynomials with distinct roots had already served to factor integers in the 1970’s. Knowing that  $\sim n^{1/4}$  operations in  $\mathbb{Z}_n$  suffice to evaluate the polynomial  $\prod_{i=1}^{i=n^{1/4}} (x - i) \in \mathbb{Z}_n[x]$  at the  $n^{1/4}$  points  $n^{1/4}, 2n^{1/4}, 3n^{1/4}, \dots, n^{1/2}$  [BoMo74], Strassen had noted [St76] that  $\log_2 n$ -bit integers can be factored deterministically in time  $\sim n^{1/4}$  with no sophisticated appeal to number theory. (This is described as the Pollard-Strassen algorithm in [GaGe03] and was also known to Borodin [Bo07]; even today, no better provable upper bound on the running time of a deterministic factoring algorithm is known.)

---

*1998 ACM Subject Classification:* F.2.1, F.1.3, I.1.1?

*Key words and phrases:* Arithmetic Circuits, Addition Chain, Prouhet-Tarry-Escott Problem, Zeros of Polynomials, Integer Factoring.

The significance of the  $\tau$ -conjecture extends beyond the prospect of its failure possibly leading to efficient integer factoring algorithms: if the conjecture holds, then  $P_{\mathbb{C}} \neq NP_{\mathbb{C}}$  in the Blum-Shub-Smale model of computation over the reals [BCSS97]. Smale therefore suggested the  $\tau$ -conjecture, in the form *there exist universal constants  $\alpha$  and  $\beta$  such that any polynomial  $f(x) \in \mathbb{Z}[x]$  has no more than  $\alpha \cdot \tau(f)^\beta$  distinct integer zeros*, as the fourth most important mathematical challenge left open at the turn of the millennium [Sm00]. Smale [Sm00] reports private communications with Schönhage, Shub and Bürgisser extracting from Strassen’s work that  $\beta$  in the  $\tau$  conjecture has to be at least 2, yet Rojas [Ro03] mentions that the case  $\beta = 1$  is still open.

Bürgisser [Bu01] extended the  $\tau$ -conjecture to arbitrary number fields and further allowed any base ring elements as circuit inputs. Bürgisser conjectured that for some  $\beta$ , any polynomial  $f(x) \in \mathbb{Q}[x]$  has at most  $(L(f) + d)^\beta$  irreducible factors of degree at most  $d$ , where  $L(f)$  is the size of a smallest  $\{+, -, \times, \div\}$ -circuit computing  $f(x)$  from  $\{x\} \cup \mathbb{Q}$ . Bürgisser’s conjecture became known as the  $L$ -conjecture, and it clearly implies the  $\tau$ -conjecture.

A weakened  $L$ -conjecture was studied by Cheng [Ch04]. Cheng showed that if true, his conjecture would improve and yield an independent proof of recent results concerning elliptic curves. The  $L$ -conjecture implies Cheng’s weaker version, but the connection between Cheng’s conjecture and the  $\tau$ -conjecture is unclear. See Cheng [Ch04] and [Ro03] for an account of the history and for the latest results, including the observation that no significant progress has been reported on the  $\tau$ -conjecture itself, and the best known upper bound [Ro03] on the number of roots as a function of the number of additive gates.

The present paper derives from empirical work concerning integer polynomials of degree  $2^n$  for  $n = 1, 2, 3, 4$ . For these values of  $n$  we managed to combine  $n$  product gates and  $n$  addition gates into circuits that compute, from the input  $x$  and carefully selected integer inputs, polynomials  $p(x) \in \mathbb{Z}[x]$  of degree  $2^n$  having  $2^n$  distinct roots in  $\mathbb{Z}$ . So we ask:

*Do such phenomenally efficient circuits exist for every  $n$ ?*

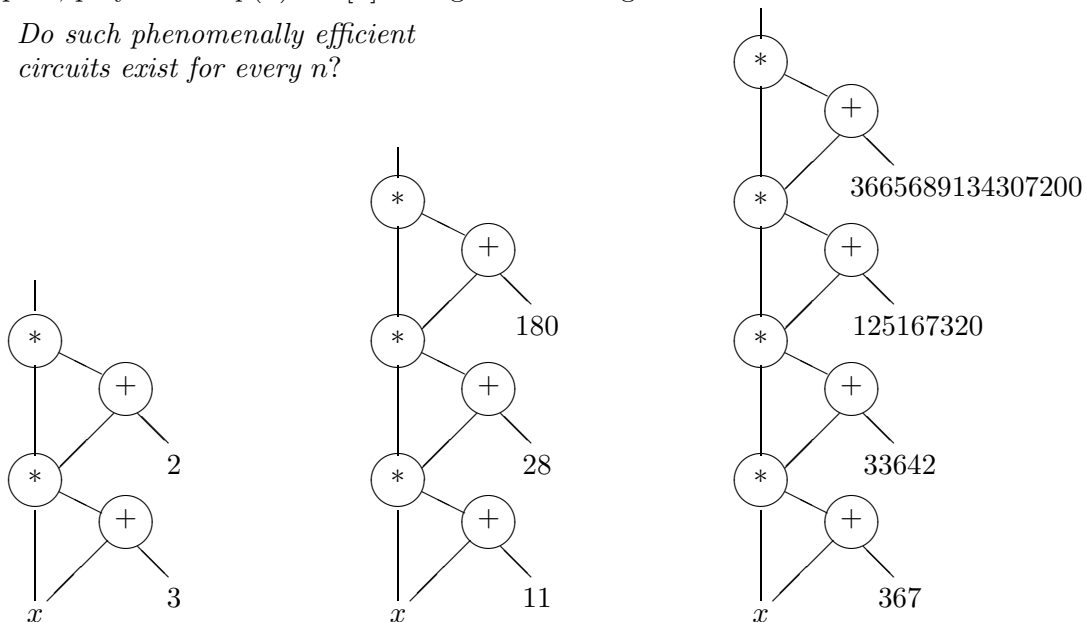


Figure 1: The leftmost circuit has zeros  $0, -1, -2, -3$ , the second one has zeros  $0, -1, -2, -4, -7, -9, -10, -11$  and the third one has zeros  $0, -4, -7, -12, -118, -133, -145, -178, -189, -222, -234, -249, -355, -360, -363, -367$ .

A positive answer would disprove the  $L$ -conjecture in a strong sense. A negative answer would constitute a modest first step towards proving it. Our initial expectation was to readily dispose of the question. Yet we cannot resolve it.

If  $c$  is a  $\{+, -, \times\}$ -circuit (see Section 2) with inputs from  $\{x\} \cup \mathbb{Z}$ , we will write

- $c_+$  for the total number of *additive*, i.e. addition or subtraction, gates in  $c$ ,
- $c_\times$  for the total number of product gates in  $c$ ,
- $f_c(x) \in \mathbb{Z}[x]$  for the polynomial computed by  $c$ ,
- $\text{izeros}_c$  for  $\{a \in \mathbb{Z} : f_c(a) = 0\}$ .

We will say that

- $c$  is a  $d$ -gem, where  $d$  is any positive integer, if  $d = |\text{izeros}_c| = \deg(f_c(x))$  and  $c_\times \leq \ell_d$ , where  $\ell_d$  is the length of a shortest addition chain for  $d$ , which is the same as the size of a  $(1,+)$ -circuit,
- $c$  is *skew* if every additive gate in  $c$  has one input from  $\mathbb{Z}$ ,
- $c$  is an *optimal  $d$ -gem* (resp. an *optimal skew  $d$ -gem*) if  $c$  is a  $d$ -gem provably having a minimal number of additive gates among all  $d$ -gems (resp. among all skew  $d$ -gems).

Hence a  $2^n$ -gem is a  $\{+, -, \times\}$ -circuit with  $n$  product gates that computes a polynomial of maximum degree  $2^n$  and this polynomial factors completely with its  $2^n$  roots integer and distinct. The examples in Figure 1 are  $2^n$ -gems which are optimal skew. If  $d$ -gems exist for infinitely many  $d$ , then the  $L$ -conjecture fails (Proposition 1.3).

The contributions of this paper are the following:

- we construct skew  $d$ -gems for  $d \leq 22$  (see Figure 2);
- we construct  $d$ -gems for  $d = 24, 25, 26, 27, 28, 29, 30, 31, 36, 37, 42, 54, 55$  (see Fig. 2);
- we show that for  $d \leq 71$ ,  $d$ -gems require  $\ell_d$  product gates; we conclude that all the  $d$ -gems we are able to construct have a minimal number of product gates;
- we show that a skew  $2^n$ -gem can be *normalized*, that is,  $c$  can be transformed into another skew  $2^n$ -gem  $c'$  such that the first gate of  $c'$  computes  $x \times x$  and there are  $2n - 1$  successive other gates that alternate between adding a constant and squaring;
- we observe that skew  $2^n$ -gems for  $n \geq 5$  would provide new solutions of size  $2^{n-1}$  to the Prouhet-Tarry-Escott problem of number theory, a problem with an almost 200-year history (see for instance [BoIn94]); we spell out the extra conditions that a PTE solution would have to verify for it to yield a  $2^n$ -gem in return;
- we construct skew  $d$ -gems *over the reals*, i.e. with inputs from  $\mathbb{R} \cup \{x\}$  and the requirement of distinct roots in  $\mathbb{R}$ , for every  $d$ ;
- we prove that any skew  $2^n$ -gem *over the reals* requires at least  $n$  additive gates; we conclude that our skew  $2^n$ -gems (over  $\mathbb{Z}$ ) for  $n = 1, 2, 3, 4$  are optimal.

## 1. Formal definitions and preliminaries

An *arithmetic circuit* is a rooted directed acyclic graph with in-degree-2 nodes called *gates* labeled by  $\times, +, -$  and in-degree-0 nodes labeled by integer constants and variables. In this paper we only consider univariate polynomials. An arithmetic circuit  $c$  represents a polynomial  $f_c(x) \in \mathbb{Z}[x]$ . A *zero* or *root* of  $c$  is an integer zero of the polynomial  $f_c(x)$ , i.e. an integer  $a$  such that  $f_c(a) = 0$ . For example, the circuit  $c$  shown on the left of Figure 1 has  $c_\times = 2$  product gates, it has  $c_+ = 2$  additive gates and it represents the degree-4 polynomial  $f_c(x) = (x(x+3))(x(x+3)+2) = x^4 + 6x^3 + 11x^2 + 6x$ . This polynomial is easily seen to have the set  $\text{izeros}_c = \{0, -1, -2, -3\}$  of integer zeroes.

$d$	$c_{\times}$	$c_{+}$	$f_c(x)$	$\text{izeros}_c$
1	0	0	$x$	$\{0\}$
2	1	1	$x^2 - 1$	$\{-1, 1\}$
3	2	1	$(x^2 - 1)x$	$\{-1, 0, 1\}$
4	2	2	$((x^2 - 5)^2 - 16)$	$\{-1, 1, -3, 3\}$
5	3	2	$((x^2 - 5)^2 - 16)x$	$\{0, -2, 2, -3, 3\}$
5	3	2	$(x^2 - 1)((x^2 - 4)x)$	$\{0, -1, 1, -2, 2\}$
6	3	2	$((x^2 - 25)^2 - 24^2)(x^2 - 25)$	$\{-1, 1, -7, 7, -5, 5\}$
6	3	2	$((x^2 - 7)x)^2 - 36$	$\{1, 2, -3, -1, -2, 3\}$
7	4	2	$((x^2 - 7)x)^2 - 36)x$	$\{0, -1, 1, -2, 2, -3, 3\}$
7	4	2	$((x^2 - 25)^2 - 24^2)(x^2 - 25)x$	$\{0, -1, 1, -7, 7, -5, 5\}$
8	3	3	$((x^2 - 65)^2 - 1696)^2 - 207360$	$\{-3, 3, -11, 11, -7, 7, -9, 9\}$
9	4	2	$((x^2 - 49)x)^2 - 120^2)((x^2 - 49)x)$	$\{0, -3, 3, -5, 5, -8, 8, -7, 7\}$
10	4	3	$((y^2 - 236448)^2 - 123552^2)y$ with $y = (x^2 - 625)$	$\{-5, -35, -17, -31, -25, 5, 35, 17, 31, 25\}$
10	4	3	$((x^2 - 250)^2 - 14436)x^2 - 1612802$	$\{-4, -8, 14, 18, -20, 4, 8, -14, -18, 20\}$
11	5	3	The above $\times x$	$\{0, -5, -35, -17, -31, -25, 5, 35, 17, 31, 25\}$
12	4	3	$((x^2 - 91)x)^2 - 58500^2 - 50400^2$	$\{-1, -9, 10, 1, 9, -10, -5, -6, 11, 5, 6, -11\}$
13	5	3	The above $\times x$	The above $\cup \{0\}$
14	5	3	$((x^2 - 7^4)x)^2 - \dots)^2 - \dots)(x^2 - 7^4)$	$\{\pm 49, 16, 39, 55, 21, 35, 56\}$
15	5	3	$y \times (y^2 - 34320^2) \times (y^2 - 41160^2)$ with $y = (x^2 - 7^4)x$	$\{\pm 0, 49, 16, 39, 55, 21, 35, 56\}$
16	4	4	$((x^2 - 67405)^2 - \dots)^2 - \dots$	$\{\pm 11, 367, 131, 343, \pm 77, 359, 101, 353\}$
17	5	4	The above $\times x$	The above $\cup \{0\}$
18	5	5	$f_{c_{16}} \cdot (x^2 - 1)$	$\{\pm 1, 11, 367, 131, 343, 77, 359, 101, 353\}$
18	5	4	$(y^2 - 2484^2) \times (y^2 - 4116^2) \times (y^2 - 5916^2)$ with $y = (x^2 - 7^2 \cdot 13)x$	$\{\pm 4, 23, 27, 7, 21, 27, 12, 17, 29\}$
19	6	4	The above $\times x$	The above $\cup \{0\}$
20	5	5	$f_{c_{16}} \cdot ((x^2 - 67405)^2 - 3958423056)$	$\{\pm 67, 361, 11, 367, 131, 343, 77, 359, 101, 353\}$
21	6	4	$y \times (y^2 - 89760^2) \times (y^2 - 150480^2) \times$ $(y^2 - 263640^2)$ with $y = (x^2 - 7^2 \cdot 13^2)x$	$\{\pm 0, 91, 11, 85, 96, 19, 80, 99, 39, 65, 104\}$
22	6	6	$f_{c_{20}} \cdot (x^2 - 1)$	$\{\pm 1, 67, 361, 11, 367, 131, 343, 77, 359, 101, 353\}$
23	has the unique minimal chain 1, 2, 3, 5, 10, 20, 23 and we have been unable to find a 23-gem so far.			
24	5		$f_{c_4}(y^2)$ with $y = (x^2 - 7 \cdot 13 \cdot 19)x$	$\{\pm 3, 40, 43, 8, 37, 45, 15, 32, 47, 23, 25, 48\}$
24	5	442	$z(z + c_{Prop.2.10})$ with $y = (x^2 - 11763)^2$ and $z = (y + 241x^2 + ..)(y + 195x^2 + ..)(y + x^2 + ..)$	$\{\pm 22, 61, 86, 127, 140, 151,$ $35, 47, 94, 121, 146, 148\}$
26	6	443	$f_{c_{24}} \cdot (x^2 - 1)$	$\text{Set}_{24} \cup \{-1, 1\}$
27	6		$y \times f_{c_4}(y^2)$ with $y = (x^2 - 7^2 \cdot 13^2)x$	$\text{Set}_{21} \cup \{\pm 49, 56, 105\}$
28	6	560	$f_{c_{24}} \cdot (y + 117x^2 + \dots)$	$\text{Set}_{24} \cup \{-1, 1, -153, 153\}$
30	6		$f_{c_5}(y^2)$ with $y = (x^2 - 7^2 \cdot 13^2 \cdot 19)x$	$\{\pm 13, 390, 403, 35, 378, 413, 70, 357, 427,$ $103, 335, 438, 117, 325, 442\}$
36	6		$f_{c_6}(y^2)$ with $y = (x^2 - 7^2 \cdot 13^2 \cdot 19)x$	$\text{Set}_{30} \cup \{\pm 137, 310, 447\}$
42	7		$f_{c_7}(y^2)$ with $y = (x^2 - 7^2 \cdot 13^2 \cdot 19)x$	$\text{Set}_{36} \cup \{\pm 182, 273, 455\}$
54	7		$f_{c_9}(y^2)$ with $y = (x^2 - 7^2 \cdot 13^2 \cdot 19)x$	$\text{Set}_{42} \cup \{\pm 202, 255, 457, 225, 233, 458\}$
55	8		The above $\times x$	The above $\cup \{0\}$

Figure 2: Some skew  $d$ -gems for  $d \leq 22$ . When two examples are given for a given  $d$ , these arise from different minimal addition chains for  $d$ . The functions  $f_{c_i}$  are from Lemma 3.2 if  $i \leq 9$  and from the  $i$ -gem in this table otherwise. Constructions are explained in the text or the appendix. We omitted the cases  $d = 25, 29, 31, 37$  which, like the case  $d = 55$  here, are obtained by extending a  $(d - 1)$ -gem; we note that such an extension does not work for 43 which has a shorter addition chain not using the 42.

An *addition chain* for a natural number  $d$  is an increasing sequence  $d_0 = 1, d_1, \dots, d_k = d$  of natural numbers such that each  $d_i$  for  $i > 0$  is the sum of two earlier numbers in the sequence. We write  $\ell_d$  for the minimal  $k$  such that there is an addition chain such that  $d_k = d$ . The polynomial  $x^d$  is computable by a circuit having  $\ell_d$  product gates (see [Kn81] for extensive related facts on addition chains).

**Definition 1.1.** A  $d$ -gem is a circuit  $c$  such that  $d = |\mathbf{zeros}_c| = \deg(f_c(x))$  and  $c_\times \leq \ell_d$ .

Note that we do not impose for a  $d$ -gem  $c$  that  $c_\times$  be minimal, although this follows when  $d = 2^n$  for some  $n$  since then

$$2^{\ell_{2^n}} = 2^n = d = |\mathbf{zeros}_c| = \deg(f_c(x)) \leq 2^{c_\times} \leq 2^{\ell_d} = 2^{\ell_{2^n}},$$

implying that  $c_\times = \ell_d$  is the only choice in that case. It is an amazing prospect, brought to our attention by Allan Borodin, that unpublished work by Strassen might have uncovered circuits  $c$  with  $c_\times < \ell_{\deg(f_c(x))}$ . For that reason, our requirement on  $d$ -gems is “ $c_\times \leq \ell_d$ ” rather than “ $c_\times = \ell_d$ ” or “ $c$  is  $\{\times\}$ -optimal”. Nonetheless we can show the following, which implies that all  $d$ -gems constructed in this paper have a minimal number of product gates, since  $d < 71$  implies  $d > 2^{d-3}$  (see [Kn81, P. 446]).

**Lemma 1.2.** *If  $d > 2^{d-3}$ , then any  $\{\times, +, -\}$ -circuit computing a polynomial of degree  $d$  requires at least  $\ell_d$  product gates.*

**Proposition 1.3.** *If  $d$ -gems exist for infinitely many values of  $d$ , then the  $L$ -conjecture fails.*

## 2. $d$ -gems when $d$ is a power of 2

In this section we first develop sufficient conditions for the existence of a skew  $2^n$ -gem. Then we construct  $2^n$ -gems systematically for  $n \leq 3$ , and by computer search for  $n = 4$ . For  $n \geq 5$ , it is neither known whether our sufficient conditions can be met nor whether  $2^n$ -gems exist.

**Lemma 2.1.** *Let  $T_n(a_1, a_2, \dots, a_{2^n})$  be the full binary tree of height  $n \geq 2$  in which the leaf  $j$  for  $1 \leq j \leq 2^n$  is labeled  $a_j \in \mathbb{Z}$  and each internal node  $v$  is labeled with the product of the labels of the leaves subtended by  $v$ . Suppose that for  $1 < i < n$ , each of the  $2^i$  nodes at level  $i$  has the same “litter sum”, where the “litter sum” of a node is the sum of the labels of its two children. Then the skew circuit  $c$  below (expressed as a straight-line program),*

$$\begin{aligned} y_0 &\leftarrow x - a_1 \\ y_1 &\leftarrow y_0 \times (y_0 + (a_1 - a_2)) \\ y_2 &\leftarrow y_1 \times (y_1 + (a_3 a_4 - a_1 a_2)) \\ y_3 &\leftarrow y_2 \times (y_2 + (a_5 a_6 a_7 a_8 - a_1 a_2 a_3 a_4)) \\ &\vdots \\ &\vdots \\ y_n &\leftarrow y_{n-1} \times (y_{n-1} + (\prod_{i=2^{n-1}+1}^{2^n} a_i - \prod_{i=1}^{2^{n-1}} a_i)), \end{aligned}$$

computes the polynomial  $p(x) = \prod_{1 \leq i \leq 2^n} (x - a_i)$ .

*Proof.* When  $n = 2$  the circuit correctly computes  $p(x) = y_1(x) = (x - a_1)(x - a_1 + (a_1 - a_2))$ . For the inductive step, we can write

$$\begin{aligned} p(x) &= [(x - a_1)(x - a_2)] \times [(x - a_3)(x - a_4)] \times \cdots \times [(x - a_{2^{n-1}})(x - a_{2^n})] \\ &= [x^2 - (a_1 + a_2)x + a_1a_2] \times [x^2 - (a_3 + a_4)x + a_3a_4] \cdots [x^2 - (a_{2^{n-1}} + a_{2^n})x + a_{2^{n-1}}a_{2^n}] \\ &= [x^2 - (a_1 + a_2)x + a_1a_2] \times [x^2 - (a_1 + a_2)x + a_3a_4] \cdots [x^2 - (a_1 + a_2)x + a_{2^{n-1}}a_{2^n}] \end{aligned}$$

since each node at level  $n - 1$  in  $T_n(a_1, a_2, \dots, a_{2^n})$  has the litter sum  $a_1 + a_2$ . Letting  $y = x^2 - (a_1 + a_2)x$ ,

$$\begin{aligned} p(x) &= (y + a_1a_2) \times (y + a_3a_4) \times \cdots \times (y + a_{2^{n-1}}a_{2^n}) \\ &= q(y). \end{aligned}$$

Now the litter sum conditions imposed by the tree  $T_{n-1}(-a_1a_2, -a_3a_4, \dots, -a_{2^{n-1}}a_{2^n})$  are identical to the litter sum conditions imposed by the top part  $T_{n-1}(a_1a_2, a_3a_4, \dots, a_{2^{n-1}}a_{2^n})$  of  $T_n(a_1, a_2, \dots, a_{2^n})$ . Hence by induction, the circuit

$$\begin{aligned} z_0 &\leftarrow y - (-a_1a_2) \\ z_1 &\leftarrow z_0 \times (z_0 + (-a_1a_2 - (-a_3a_4))) \\ z_2 &\leftarrow z_1 \times (z_1 + (a_5a_6a_7a_8 - a_1a_2a_3a_4)) \\ &\vdots \\ &\vdots \\ z_{n-1} &\leftarrow z_{n-2} \times (z_{n-2} + (\prod_{i=2^{n-2}+1}^{2^{n-1}} a_i - \prod_{i=1}^{2^{n-2}} a_i)) \end{aligned}$$

computes the polynomial  $q(y)$ . Now one checks that  $z_0 = y - (-a_1a_2) = y_1$  and  $z_1 = z_0 \times (z_0 + (-a_1a_2 - (-a_3a_4))) = y_2$ , from which it follows that for  $0 \leq i \leq n - 1$ ,  $z_i = y_{i+1}$ . ■

## 2.1. 2-gems and 4-gems

For any  $a_1 < a_2 < a_3 < a_4 \in \mathbb{Z}$  there is a 2-gem computing  $(x - a_1)(x - a_2)$ , and the 4-gem

$$\begin{aligned} y_0 &\leftarrow x - a_1 \\ y_1 &\leftarrow x - a_2 \\ y_2 &\leftarrow y_0 \times y_1 \\ y_3 &\leftarrow y_2 + \underbrace{x + x + \cdots + x}_{a_1 + a_2 - a_3 - a_4 \text{ times}} + (a_3a_4 - a_1a_2) \\ y_4 &\leftarrow y_2 \times y_3 \end{aligned}$$

computes  $p(x) = (x - a_1)(x - a_2)(x - a_3)(x - a_4)$ . Alternatively, when the litter sum conditions from  $T_4(a_1, a_4, a_2, a_3)$  are fulfilled, namely when  $a_1 + a_4 = a_2 + a_3$ , Lemma 2.1 yields a much more efficient (skew) 4-gem for  $p(x)$ , having only 3 additive gates. We thus record:

**Proposition 2.2.** *For any  $a_1 < a_2 < a_3 < a_4 \in \mathbb{Z}$ , there is a 4-gem computing  $\prod_{i=1}^4 (x - a_i)$ , and if  $a_1 + a_4 = a_2 + a_3$  then a skew 4-gem with 3 additive gates (2 additive gates if  $a_1 = 0$ ) computes it.*

## 2.2. 8-gems

Not all polynomials  $p(x) \in \mathbb{Z}[x]$  of degree 8 having 8 distinct roots seem to have an 8-gem. But we can construct an 8-gem by prepending “ $y \leftarrow x \times x$ ” to the 4-gem for the polynomial  $q(y) = (y - a^2)(y - b^2)(y - c^2)(y - d^2)$  available by Proposition 2.2. If  $a^2 + d^2 = b^2 + c^2$ , then Proposition 2.2 further yields a skew 4-gem with 3 additive gates for  $q(y)$ , proving:

**Proposition 2.3.** *For any  $0 < a^2 < c^2 < d^2 < b^2 \in \mathbb{Z}$ , there is an 8-gem computing the polynomial  $p(x) = (x - a)(x + a)(x - b)(x + b)(x - c)(x + c)(x - d)(x + d)$ , and if  $a^2 + b^2 = c^2 + d^2$  then a skew 8-gem with 3 additive gates computes it.*

We note in the following that distinct  $a, b, c, d$  fulfilling  $a^2 + b^2 = c^2 + d^2$  abound.

**Proposition 2.4.** *If  $p = e^2 + f^2$  and  $q = g^2 + h^2$  are distinct primes, then  $a = |eg + fh|$ ,  $b = |eh - fg|$ ,  $c = |eg - fh|$  and  $d = |eh + fg|$  are distinct integers verifying*

$$a^2 + b^2 = c^2 + d^2.$$

**Corollary 2.5.** *There are infinitely many sets  $\{a^2, b^2, c^2, d^2\}$  of 4 distinct non-zero squares such that a skew 8-gem exists computing  $(x - a)(x + a)(x - b)(x + b)(x - c)(x + c)(x - d)(x + d)$  using 3 additive gates.*

## 2.3. 16-gems

We constructed skew 16-gems by using a computer to search for skew 8-gems computing  $q(y) = (y - a^2)(y - b^2)(y - c^2)(y - d^2)(y - e^2)(y - f^2)(y - g^2)(y - h^2)$ . A 16-gem is obtained at no extra additive cost from such an 8-gem by prepending it with “ $y \leftarrow x \times x$ ”. To obtain a skew 8-gem for  $q(y)$ , we exploited Lemma 2.1. The litter sum conditions from  $T_8(a^2, b^2, c^2, d^2, e^2, f^2, g^2, h^2)$  are then

$$\begin{aligned} a^2 + b^2 &= c^2 + d^2 = e^2 + f^2 = g^2 + h^2 \\ (ab)^2 + (cd)^2 &= (ef)^2 + (gh)^2. \end{aligned}$$

By running a small computer for several hours, we found several examples of sequences of numbers fulfilling the above litter sum conditions. In particular:

**Proposition 2.6.** *A 16-gem with 4 additive gates exists to compute the polynomial of degree 16 having the 16 roots  $\{\pm 237, \pm 106, \pm 189, \pm 178, \pm 227, \pm 127, \pm 218, \pm 141\}$ .*

The Appendix contains other 16-gem examples, some obtained by a variant of Lemma 2.1.

## 2.4. Normal form for $2^n$ -gems

**Definition 2.7.** A  $2^n$ -gem  $c$  is *normalized* if it is skew, it contains no subtraction gate,  $c_+ = c_\times (= n)$ , and  $\times$ -gates and  $+$ -gates alternate along every path from  $x$  to the output gate, which is a  $+$ .

Note that the graph of a normalized  $2^n$ -gem depends only on  $n$ , since every path from  $x$  to the output gate must encounter every  $\times$ -gate for the degree of  $f_c(x)$  to reach  $2^n$ , and alternation implies that every such path encounters every  $+$ -gate as well. Hence, starting from  $x$ , a normalized  $2^n$ -gem repeatedly squares and adds an integer. A normalized  $2^n$ -gem is thus entirely described by a sequence of  $n$  integers.

**Lemma 2.8.** (Normal form) Given  $a_1, \dots, a_{2^n} \in \mathbb{Z}$  and a skew  $2^n$ -gem computing the polynomial  $\prod_{i=1}^{2^n} (x - a_i)$ , there exist  $s \in \mathbb{Z}$  and  $t \in \{1, 2\}$  such that the polynomial  $\prod_{i=1}^{2^n} (x - t(a_i + s))$  is computed by a normalized  $2^n$ -gem.

## 2.5. $2^n$ -gems and the Prouhet-Tarry-Escott problem

**Definition 2.9.** (see [BoIn94]) Two sets  $\{a_1, \dots, a_m\}, \{b_1, \dots, b_m\}$  solve to the Prouhet-Tarry-Escott problem (PTE) of degree  $k$  if  $a_1^i + \dots + a_m^i = b_1^i + \dots + b_m^i$  for all  $i \leq k$ . A solution is called ideal if  $k = m - 1$ . A solution of the form  $\{a_1, -a_1, \dots, a_{m/2}, -a_{m/2}\}, \{b_1, -b_1, \dots, b_{m/2}, -b_{m/2}\}$  is called symmetric and we abbreviate it by  $\{a_1, \dots, a_{m/2}\}, \{b_1, \dots, b_{m/2}\}$ .

The following proposition will serve to relate gems and PTEs. This proposition is an “elementary property”, stated as Proposition 1 in [BoIn94] and known at least since [DoBr37]. Let  $p(x) = (x - a_1)(x - a_2) \cdots (x - a_m)$  and  $q(x) = (x - b_1)(x - b_2) \cdots (x - b_m)$ . Define, for  $k = 1, 2, \dots, m$ ,  $s_k = \sum_{i=1}^m a_i^k$  and  $t_k = \sum_{i=1}^m b_i^k$ .

**Proposition 2.10.** (Well known, see [BoIn94].) *The following are equivalent:*

- $s_1 = t_1$  and  $s_2 = t_2$  and  $s_3 = t_3$  and  $\dots$  and  $s_k = t_k$
- $\text{degree}[p(x) - q(x)] \leq m - (k + 1)$ .

**Corollary 2.11.** *For any  $n \geq 1$  and any skew  $2^n$ -gem  $c$  such that  $\text{izeros}_c = \{a_1, \dots, a_{2^n}\}$ , there is a partition  $S \uplus T = \{a_1, \dots, a_{2^n}\}$  such that the pair  $S, T$  is an ideal PTE solution of size  $2^{n-1}$ .*

*Proof.* We first apply Lemma 2.8 to normalize  $c$ . The result is a circuit  $c'$  computing a polynomial  $\prod_{i=1}^{2^n} (x - t(a_i + s))$  for some  $s \in \mathbb{Z}$  and  $t \in \{1, 2\}$ . This polynomial equals  $(r(x))^2 - e$  for some polynomial  $r(x)$ , where  $e \in \mathbb{N}$  results from the last addition in  $c'$ . Now  $(r(x))^2 - e = p(x)q(x)$ , where  $p(x) = (r(x) + \sqrt{e})$  and  $q(x) = (r(x) - \sqrt{e})$ . Since  $\mathbb{Z}[x]$  is a Euclidian ring,  $p(x)$  and  $q(x)$  must each have  $2^{n-1}$  distinct roots. (Thus  $\sqrt{e} \in \mathbb{N}$ .) The degree of  $p(x) - q(x)$  is 0, so applying Proposition 2.11 with  $k = m - 1$  shows that the roots of  $p(x)$  and the roots of  $q(x)$  form an ideal PTE solution of size  $2^{n-1}$ . Dividing out everywhere by  $t$  yields another PTE solution, and it is well known [BoIn94] that shifting from  $a_i + s$  back to  $a_i$  also preserves PTE solutions. ■

The example on the right side of Figure 5 leads to the symmetric ideal solution

$$\{212, 356, 388, 474\}, \{352, 282, 454, 436\}.$$

This solution has the additional property that  $212^2 + 474^2 = 269620 = 356^2 + 388^2$ . Now, can we go the other way around and construct  $2^n$ -gems from PTE solutions? Consider the ideal symmetric solution  $\{2, 16, 21, 25\}, \{5, 14, 23, 24\}$  (from [BoIn94]). We would have to express  $p(x) = (x^2 - 2^2)(x^2 - 16^2)(x^2 - 21^2)(x^2 - 25^2)$  using 3 products. This could be done by calculating  $(x^2 - 2^2)(x^2 - 25^2)$  using 2 products, then forming  $(x^2 - 16^2)(x^2 - 21^2)$  from  $(x^2 - 2^2)(x^2 - 25^2)$  (where repeated additions of  $x^2$  would be necessary because  $2^2 + 25^2 \neq 16^2 + 21^2$ ), and finally obtaining  $p(x)$  using one last product. Thus the 16-gems obtained from the PTE would not be skew.

Section 3 will expand on the usefulness of PTEs, for example constructing a 24-gems from a PTE solution of degree 12. But even if PTE solutions of degree 16 were known, we would need additional properties to exploit the above idea in constructing a 32-gem.

Naturally, conditions stronger than those afforded by ideal PTE solutions do imply skew  $2^n$ -gems. We give a concise description of these now.

**Definition 2.12.** A pair of sets of the form  $\{a_1, -a_1, \dots, a_{m/2}, -a_{m/2}\}, \{b_1, -b_1, \dots, b_{m/2}, -b_{m/2}\}$  is called *sym-perfect* if either  $m = 2$ , or there exists  $s \in \mathbb{Z}$  such that  $\{a_1^2 + s, \dots, a_{m/2}^2 + s\}, \{b_1^2 + s, \dots, b_{m/2}^2 + s\}$  is sym-perfect.

If we assume w.l.o.g. that  $a_1^2$  is the smallest and  $a_{m/2}^2$  is the biggest number in  $\{a_1^2, \dots, a_{m/2}^2\}$ , then the shift  $s$  occurring in the recursive definition of sym-perfect is necessarily equal to  $-(a_1^2 + a_{m/2}^2)/2$  (which is also the average of all the numbers that occur).

An example of a sym-perfect pair is  $\{-3, 3, -11, 11\}, \{-7, 7, -9, 9\}$ , since  $\{9 - 65, 121 - 65\}, \{49 - 65, 81 - 65\}$  is sym-perfect.

**Theorem 2.13.** *A pair  $\{a_1, -a_1 \dots a_{2^n/2}, -a_{2^n/2}\}, \{b_1, -b_1, \dots, b_{2^n/2}, -b_{2^n/2}\}$  is sym-perfect if and only if the numbers involved are the zeros of a normalized  $2^{n+1}$ -gem.*

*Proof:* The pair  $\{(a_1^2 - b_1^2)/2\}, \{(b_1^2 - a_1^2)/2\}$  corresponds to the 2-gem  $c$  with  $f_c(x) = x^2 - ((a_1^2 - b_1^2)/2)^2$  and  $\mathbf{zeros}_c = \{(a_1^2 - b_1^2)/2, (b_1^2 - a_1^2)/2\}$  for  $n = 1$ , where  $s = -(a_1^2 - b_1^2)/2$ . Assume by induction that the pair  $\{a_1^2 - s, \dots, a_{2^n/2}^2 - s\}, \{b_1^2 - s, \dots, b_{2^n/2}^2 - s\}$  corresponds to the  $2^n$ -gem  $c$  with  $\mathbf{zeros}_c = \{a_1^2 - s, \dots, a_{2^n/2}^2 - s, b_1^2 - s, \dots, b_{2^n/2}^2 - s\}$ , then the pair  $\{a_1, -a_1 \dots a_{2^n/2}, -a_{2^n/2}\}, \{b_1, -b_1, \dots, b_{2^n/2}, -b_{2^n/2}\}$  corresponds to the  $2^{n+1}$ -gem  $c'$  with  $f_{c'}(x) = f_c(x^2 - s)$  with  $\mathbf{zeros}'_{c'} = \{a_1, -a_1 \dots a_{2^n/2}, -a_{2^n/2}, b_1, -b_1, \dots, b_{2^n/2}, -b_{2^n/2}\}$ . Since the powers in odd PTE-equations cancel in a symmetric pair and the even PTE-equations follow by recursion, we get the following corollary giving us an alternative proof for Corollary 2.11:

**Corollary 2.14.** *A sym-perfect pair is an ideal, symmetric PTE solution.*

## 2.6. Skew $2^n$ -gems require $n$ additive gates

We already noted that a circuit  $c$  representing a polynomial  $f_c$  with  $2^n$  distinct integer zeros needs  $\geq n$  multiplications. In the following we will show that if  $c$  has exactly  $n$  multiplications and  $c$  is skew, then  $c$  needs  $\geq n$  additive gates. We are able to prove this because the result holds over the real numbers.

Let  $A$  be  $\mathbb{Z}, \mathbb{Q}$  or  $\mathbb{R}$ . For short, we will say that a nonzero polynomial  $p(x) \in \mathbb{R}[x]$  *crumbles over  $A$*  if  $\deg(p) = 0$  or if  $p$  has  $\deg(p)$  distinct roots in  $A$ .

**Proposition 2.15.** *Let  $A$  be  $\mathbb{Z}, \mathbb{Q}$  or  $\mathbb{R}$ . Let  $p(x) \in \mathbb{R}[x]$  and  $q(x) \in \mathbb{R}[x]$ . If  $pq$  crumbles over  $A$  then both  $p$  and  $q$  crumble over  $A$ .*

**Proposition 2.16.** *(Rolle) Over  $\mathbb{R}$ , the derivative of a crumbling polynomial crumbles.  $\square$*

Note that Rolle only applies over  $\mathbb{R}$ . For example,  $(x-1)(x-2)(x-3)$  crumbles over  $\mathbb{Z}$  but its derivative  $3x^2 - 12x + 11$  crumbles neither over  $\mathbb{Z}$  nor over  $\mathbb{Q}$ . This explains our current need to work over  $\mathbb{R}$  to prove a lower bound on the number of additive gates in a  $2^n$ -gem (over  $\mathbb{Z}$ ). Recall that a  $2^n$ -gem over  $\mathbb{R}$  refers to a  $\{+, -, \times\}$ -circuit with  $n$  product gates that computes from  $\mathbb{R} \cup \{x\}$  a degree- $2^n$  polynomial  $p(x) \in \mathbb{R}[x]$  that crumbles over  $\mathbb{R}$ .

**Lemma 2.17.** *Let  $e \in \mathbb{R}$  and suppose that a polynomial  $p(x) + e \in \mathbb{R}[x]$  of degree  $2^n$  crumbles over  $\mathbb{R}$ . Then the following holds:*

**H1.** *Any skew gem over  $\mathbb{R}$  for  $p(x)$  has at least  $n - 1$  additive gates.*

**H2.** *If  $e = 0$  then any skew gem over  $\mathbb{R}$  for  $p(x)$  has at least  $n$  additive gates.*

**Theorem 2.18.** *A skew  $2^n$ -gem over the reals has at least  $n$  additive gates.*

*Proof.* This follows by applying Lemma 2.17 with  $e = 0$ . ■

**Corollary 2.19.** *Any skew  $2^n$ -gem (over  $\mathbb{Z}$ ) requires  $n$  additive gates.*

*Proof.* Let a skew gem  $c$  compute  $p(x) \in \mathbb{Z}[x]$ . Then  $c$  is also a skew gem over the reals for  $p(x)$  viewed as a real polynomial. By Theorem 2.18,  $c$  must have at least  $n$  real additive gates, hence a fortiori  $n$  integer additive gates. ■

### 3. $d$ -gems for general $d$

Example 1 in [Ro03] is a sequence of  $2^n$ -gems over the reals for any  $n$ . The following variation yields optimal  $2^n$ -gems:  $g_1 = x$  and  $g_{i+1}(x) := g_i^2(x) - 2$ ,  $1 \leq i < n$ , yields  $g_n(x) \in \mathbb{R}[x]$  having  $2^n$  distinct roots in  $[-2, 2]$ . We extend this to arbitrary degrees:

**Proposition 3.1.** *For every  $d > 0$ , there exists an optimal  $d$ -gem over the reals.*

The construction in the proof of Lemma 3.1 will lead to at most  $l_d$  additions (which occurs in the cases of  $a_i = 2^i$ ). In some cases like  $d = 3, 7, 9, 27, 81$ , we have  $l_d/2$  additions. We conjecture that  $l_d/2$  is a lower bound for the number of additions in a  $d$ -gem.

**Lemma 3.2.** *For every  $d \leq 7$  and  $d = 9$ , for every set of distinct integers  $\{a_1, \dots, a_d\}$ , there is a  $d$ -gem  $c_d$  such that  $f_{c_d}(x) = (x - a_1)(x - a_2) \cdots (x - a_d)$ .*

*Proof.* The  $d$ -gems are obtained as follows:  $f_{c_1}(x) = (x - a_1)$ ,  $f_{c_2}(x) = (x - a_1) \times (x - a_2)$ ,  
 $f_{c_3}(x) = f_{c_2}(x) \times (x - a_3)$ ,  
 $f_{c_4}(x) = f_{c_2}(x) \times (f_{c_2}(x) + (a_1 + a_2 - a_3 - a_4) \cdot x + (a_3 a_4 - a_1 a_2))$ ,  
 $f_{c_5}(x) = f_{c_4}(x) \times (x - a_5)$ ,  
 $f_{c_6}(x) = f_{c_3}(x) \times (f_{c_3}(x) + a \cdot f_{c_2}(x) + (a \cdot (a_1 + a_2) - a_1 a_2 - a_1 a_3 - a_2 a_3) \cdot x + (a_4 a_5 a_6 - a_1 a_2 a_3 - a \cdot a_1 a_2))$  with  $a = (a_1 + a_2 + a_3 - a_4 - a_5 - a_6)$ ,  
 $f_{c_7}(x) = f_{c_6}(x) \times (x - a_7)$ ,  
 $f_{c_9}(x) = f_{c_6}(x) \times (f_{c_3}(x) + a \cdot f_{c_2}(x) + (a \cdot (a_1 + a_2) - a_1 a_2 - a_1 a_3 - a_2 a_3) \cdot x + (a_7 a_8 a_9 - a_1 a_2 a_3 - a \cdot a_1 a_2))$  with  $a = (a_1 + a_2 + a_3 - a_7 - a_8 - a_9)$ ,  
■

Extending Lemma 3.2 to include  $d = 8$  would require  $a_1 + a_2 + a_3 + a_4 = a_5 + a_6 + a_7 + a_8$  since we are not able to compensate the monomial of degree 3 in  $f_{c_4}$  otherwise.

Note that the number of additive gates used in the gems from Lemma 3.2 is not minimum: We need one additive gate less if one of the zeros is 0 or if w.l.o.g.  $a_1 = -a_2$ . This allows to save two additive gates in the case of  $d \geq 3$ . For  $d \geq 4$  we have constant factors, which are regarded as a constant number of additions, for example  $|(a_1 + a_2 - a_3 - a_4)|$  additional additive gates for  $d = 4$ .

**Lemma 3.3.** *Let  $h(x) \in \mathbb{Z}[x]$  and  $m_1, m_2, \dots, m_d \in \mathbb{Z}$ . Suppose that each one of the  $d$  polynomials  $h(x) - m_i$  is computed by a gem and that no two such polynomials share a root. If  $l_d + l_{\deg(h)} \leq l_{d \cdot \deg(h)}$  and  $f_c(y) = (y - m_1)(y - m_2) \cdots (y - m_d)$  for some  $d$ -gem  $c$ , then there is a gem computing  $f_c(h(x))$ .*

*Proof.* For any  $a \in \mathbb{Z}$ ,  $f_c(h(a)) = 0$  iff  $h(a) = m_i$  for some  $i$  iff  $a$  is a root of one of the polynomials  $h(x) - m_i$ . No two such polynomials share a root and, being computed by a gem, each such polynomial has distinct roots. Hence  $f_c(h(x))$  is a polynomial of degree  $d \cdot \deg(h)$  having  $d \cdot \deg(h)$  distinct roots. To compute  $f_c(h(x))$ , we use at most  $\ell_{\deg(h)}$  product gates to compute  $h(x)$  by adding  $m_1$  to the gem for  $h(x) - m_1$ , and we use another  $\ell_d$  product gates to feed  $h(x)$  into  $c$ . In total, at most  $\ell_d + \ell_{\deg(h)}$  product gates are used, and this is at most  $\ell_{\deg(f_c(h(x)))}$  by hypothesis.  $\blacksquare$

We illustrate the use of Lemma 3.3 in the following:

**Theorem 3.4.** *There exist 36-gems and 54-gems.*

## 4. Conclusion

Lipton’s algorithm for efficiently factoring integers on average [Li94] suggests the following strategy for factoring a  $2n$ -bit integer  $N = pq$ , for primes  $p$  and  $q$  of comparable size:

- assume distinct  $a_i \in \mathbb{Z}$  and a circuit  $c$  computing  $f_c(x) = \prod_{i=1}^{2^n} (x - a_i) \in \mathbb{Z}[x]$
- pick  $a \in \{0, \dots, N - 1\}$  at random
- compute  $d = f_c(a)$  modulo  $N$  by evaluating each gate in  $c$  modulo  $N$
- output  $\gcd(d, N)$ .

This is a heuristic and not a legitimate probabilistic algorithm because its success probability depends on the distribution of the  $2^n$  integers  $(a - a_i)$  modulo  $N$ . If this is close to uniform, then indeed  $\text{Prob}[p = \gcd(d, N)] = \text{Prob}[p \text{ divides } f_c(a) \text{ but } q \text{ does not}] = \text{constant}$ . But the strategy runs in time polynomial in the number of bits required to represent  $c$ , and Smale’s  $\tau$ -conjecture [Sm00] claims that this number is exponential in  $n$ .

In this paper we introduced *gems*, ie circuits  $c$  as in the above strategy, but required to have an almost optimal number of product gates and permitted to use arbitrary size inputs. Such  $2^n$ -gems could thus serve to factor  $N$ , provided their integer inputs modulo  $N$  can be computed in time polynomial in  $n = O(\log N)$ .

We have shown that  $d$ -gems *over the real numbers* exist for every  $d$ . But the  $d$ -gems we care about (over  $\mathbb{Z}$ ) quickly run into uncharted number-theoretic territory. In particular, constructing *skew*  $2^n$ -gems for  $n \geq 5$  would yield new solutions to the Prouhet-Tarry-Escott problem. These solutions would fulfill even more than the Prouhet-Tarry-Escott conditions. Yet skew  $2^n$ -gems for  $n \geq 5$  cannot currently be ruled out. This is a measure of the current inaccessibility of  $L$ -conjecture [Bu01], since skew  $2^n$ -gems would provide the most severe counter-examples imaginable to it.

We have constructed  $d$ -gems for several small values of  $d$ , including skew  $2^n$ -gems for  $n \leq 4$  (see figures 2 and 4). We have proved that skew  $2^n$ -gems, if they exist, require  $n$  additive gates. We have shown that for  $d \leq 71$ , no circuit is able to compute a degree- $d$  polynomial using fewer than  $\ell_d$  product gates. Hence all the gems constructed so far are  $\times$ -optimal, and our  $2^n$ -gems for  $n \leq 4$  are also  $\{+, -\}$ -optimal.

Numerous open questions arise from this work, but our main open question is whether  $d$ -gems exist for every  $d$ . Perhaps a more accessible question is whether skew  $2^n$ -gems exist for  $n \geq 5$ . As seen above, constructing skew  $2^n$ -gems or disproving their existence seems like an unavoidable first step towards resolving the  $L$ -conjecture. But even this first step will apparently require serious advances in number theory.

**Acknowledgments.** We are grateful to Andrew Granville for insights and for noticing the connection between gems and the Prouhet-Tarry-Escott problem. We thank Allan Borodin for helpful suggestions, and Andreas Krebs and Klaus-Jörn Lange for useful discussions.

## References

- [BCSS97] L. Blum, F. Cucker, M. Shub and S. Smale, *Complexity and Real Computation*, Springer-Verlag, 1997.
- [Bo07] A. Borodin, private communication to [Li94] and private communication, 2007.
- [BoCo76] A. Borodin and S. Cook, On the number of additions to compute specific polynomials, *SIAM J. on Computing* 5 no. 1 (1976), pp. 146–157.
- [BoMo74] A. Borodin and B. Moenck, Fast modular transforms, *Journal of Computer and Systems Science* 8 no. 3 (1974), pp. 366–386.
- [BoIn94] A. Borwein and C. Ingalls, The Prouhet-Tarry-Escott Problem Revisited, *Enseign. Math.* **40**, 3-27, 1994.
- [Bu01] Peter Bürgisser, On implications between P-NP-Hypotheses: Decision versus computation in algebraic complexity, *Proceedings of the 26th Conference on Math. Foundations of Comp. Sci.*, Springer LNCS 2136, pp. 3-17, 2001.
- [Ch04] Q. Cheng, Straight Line Programs and Torsion Points on Elliptic Curves, *Comput. Complex.*, **12**, 3-4, Birkhauser Verlag, pp. 150–161, 2004.
- [dMSv96] W. De Melo and B. Svaiter, The cost of computing integers, *Proc. Amer. Math. Soc.* **124**, pp. 1377-1378, 1996.
- [DoBr37] H. Dolwart and O. Brown, The Tarry-Escott problem, *Proc. Amer. Math. Soc.* **44**, pp. 613-626, 1937.
- [GaGe03] J. von zur Gathen and J. Gerhard, *Modern Computer Algebra*, 2nd edition, Cambridge University Press (2003).
- [Kn81] D. Knuth, *The art of computer programming, Volume 2: Seminumerical algorithms*, 2nd ed., Addison-Wesley, 1969, 1981.
- [Li94] R. Lipton, Straight-line complexity and integer factorization, in *Algorithmic Number Theory*, LNCS 877, Springer Verlag, Berlin, pp. 71-79, 1994
- [PaSt73] M. Paterson and L. Stockmeyer, On the number of nonscalar multiplications necessary to evaluate polynomials, *SIAM J. on Computing* 2 no. 1 (1973), pp. 60–66.
- [Pa94] Chr. Papadimitriou. *Computational Complexity*. Wiley, 1994.
- [Ro03] M. Rojas, A Direct Ultrametric Approach to Additive Complexity and the Shub-Smale Tau Conjecture, <http://arxiv.org/abs/math/0304100>, 2003.
- [Ro93] K. Rosen, *Elementary number theory and its applications*, 3rd ed., Addison-Wesley, 1993.
- [Shu01] C. Shuwen, The Prouhet-Tarry-Escott Problem, <http://euler.free.fr/eslp/TarryPrb.htm>
- [Sm00] S. Smale, Mathematical problems for the next century, in V. Arnold, M. Atiyah, P. Lax and B. Mazur, editors, *Mathematics: Frontiers and Perspectives 2000*, AMS, 2000.
- [St76] V. Strassen, Einige Resultate über Berechnungskomplexität, *Jahresberichte der DMV* 78 (1976), pp. 1–8.
- [Sti95] D. Stinson. *Cryptography - Theory and Practice*. CRC Press, 1995.
- [Usp48] J. V. Uspensky. *Theory of Equations*. McGraw-Hill, 1948.
- [WIMS] [http://wims.unice.fr/wims/en\\_tool~number~twosquares.en.html](http://wims.unice.fr/wims/en_tool~number~twosquares.en.html), 1999.

## Appendix: proofs, further explanations, examples

**Lemma 1.2** If  $d > 2^{l_d-3}$ , then any  $\{\times, +, -\}$ -circuit computing a polynomial of degree  $d$  requires at least  $\ell_d$  product gates.

*Proof.* Assume there is a circuit  $c$  with a minimum number of multiplication gates to compute a polynomial of degree  $d$  but  $c_\times < \ell_d$ . Since multiplication gates can only add the degrees of their outputs and additive gates can not increase the degree, the circuit must contain an additive gate  $g$  with its output having degree  $d_1$  and its inputs having degree  $d_2 > d_1$ . This means the degree  $d_2$  is cancelled in  $g$ . Since additive gates produce only linear combinations of outputs from multiplication gates, we can assume a normal form in which additive gates are only connected in paths which have an output of a multiplication gate either only subtracted or only added. This means there must be two multiplication gates  $g_1$  and  $g_2$  producing the same degree  $d_2$ . Thus we can already estimate  $d \leq d_1 2^{c_\times^{up}} < d_2 2^{c_\times^{up}} \leq 2^{c_\times^{up}+1+c_\times^{low}} \leq 2^{c_\times-1} \leq 2^{l_d-2}$ , where each multiplication in the upper ( $c_\times^{up}$  many) and the lower part ( $c_\times^{low}$  many) of the circuit (excluding  $g_1$  and  $g_2$ ) can do one doubling. But we want a better estimation:

Let the inputs to gate  $g_1$  have the degrees  $d_3$  and  $d_4$  thus  $d_2 = d_3 + d_4$ . Assume w.l.o.g.  $d_3 \geq d_4$ . If gate  $g_2$  also has the input degrees  $d_3$  and  $d_4$ , then both gates calculate a product of the form  $(a_3x^{d_3} + \dots + a_5x^{d_5} + \dots)(a_4x^{d_4} + \dots + a_6x^{d_6} + \dots)$  where  $d_5$  and  $d_6$  are the highest degrees were the quotient  $a_3/a_5$  and  $a_4/a_6$  differ between  $g_1$  and  $g_2$ . This means the products have the form  $(a_{34}x^{d_3+d_4} + \dots + a_{45}x^{d_4+d_5} + \dots)$  or  $(a_{34}x^{d_3+d_4} + \dots + a_{36}x^{d_3+d_6} + \dots)$  and since degree  $d_3 + d_4$  is cancelled in  $g$ , the output has degree  $d_1 = d_4 + d_5$  or  $d_1 = d_3 + d_6$ . Assume w.l.o.g.  $g$  to be the highest gate in  $c$  having a reduction of the degree by cancellation. Then we can replace gate  $g_2$  by an appropriate multiple of  $g_1$  and replace  $g$  by an appropriate multiple of a new multiplication gate producing degree  $d_1 = d_4 + d_5$  or  $d_1 = d_3 + d_6$  where degrees  $d_4, d_5, d_3, d_6$  can be produced with additive gates from the lower part of the circuit. The choice of appropriate multiples (using addition gates) can avoid a cancellation in the upper part of the circuit and thus the changed circuit can produce the same degree  $d$  with the same number of multiplication gates but using no cancellation for degree  $d_1$  or above and we can repeat the whole argumentation with a smaller  $d_2$ .

Now we consider the case that  $g_2$  has different input degrees  $d'_3$  and  $d'_4$  and w.l.o.g.  $d'_3 > d_3 > d_4 > d'_4$ . With the same argument as above, there must be two multiplication gates  $g_3$  and  $g'_3$  producing either the same degree  $\geq d_3$  or producing the degrees  $d_3$  and  $d'_3$  directly. Thus we have the four gates  $g_1, g_2, g_3, g'_3$  not counted in  $c_\times^{up} + c_\times^{low} = c_\times - 4$  and we can estimate  $d \leq d_1 2^{c_\times^{up}} < d_2 2^{c_\times^{up}} < d_3 2^{c_\times^{up}+1} \leq 2^{c_\times^{up}+2+c_\times^{low}} \leq 2^{c_\times-2} \leq 2^{l_d-3}$ , contradicting the assumptions.  $\blacksquare$

Even better estimations may be obtained by further case distinctions.

**Proposition 1.3.** If  $d$ -gems exist for infinitely many values of  $d$ , then the  $L$ -conjecture fails.

*Proof.* Since  $c_\times \leq \ell_d \leq 2 \lg d$ , a  $d$ -gem  $c$  computes, even without division, a polynomial having  $d = \Omega(2^{\sqrt{c_\times}})$  distinct integer roots. To disprove the  $L$ -conjecture, we need a lower bound in terms of the *total* number of gates in the circuit. It thus suffices to argue that a  $d$ -gem  $c$  can be simulated by a  $\{\times, +, -\}$ -circuit of total size polynomial in  $c_\times$ . To do this,

we note as in [PaSt73] that for  $1 \leq i \leq c_\times$ , the  $i$ th product gate  $g$  in  $c$  computes

$$\left( \sum_{j=-1}^{i-1} a_{i,j} \mu_j \right) \times \left( \sum_{j=-1}^{i-1} b_{i,j} \mu_j \right) \quad (4.1)$$

where  $a_{i,j}, b_{i,j} \in \mathbb{Z}$ ,  $\mu_{-1} = 1$ ,  $\mu_0 = x$  and  $\mu_1, \dots, \mu_{i-1}$  are polynomials computed by earlier product gates. Hence a subcircuit of size linear in  $c_\times$  can compute (4.1) from  $\mu_{-1}, \mu_0, \dots, \mu_{i-1}$  and the integer constants. It follows that a circuit  $c'$  with  $c'_\times + c'_+ = O(c_\times^2)$  computes  $f_c(x)$ . ■

**Proposition 2.4.** If  $p = e^2 + f^2$  and  $q = g^2 + h^2$  are distinct primes, then  $a = |eg + fh|$ ,  $b = |eh - fg|$ ,  $c = |eg - fh|$  and  $d = |eh + fg|$  are distinct integers verifying

$$a^2 + b^2 = c^2 + d^2.$$

*Proof.* We apply the following identity, known as the Brahmagupta-Fibonacci equation,

$$pq = (eg + fh)^2 + (eh - fg)^2 = (eg - fh)^2 + (eh + fg)^2,$$

and show by a case analysis that  $a, b, c$  and  $d$  are distinct. ■

**Corollary 2.5.** There are infinitely many sets  $\{a^2, b^2, c^2, d^2\}$  of 4 distinct non-zero squares such that a skew 8-gem exists computing  $(x-a)(x+a)(x-b)(x+b)(x-c)(x+c)(x-d)(x+d)$  using 3 additive gates.

*Proof.* By Dirichlet's theorem on primes in arithmetic progressions (see [Ro93]), there are infinitely many primes congruent to 1 modulo 4. Now it is well known (see [Ro93, Theorem 11.4]) that any such prime can be written as a sum of two non-zero squares. ■

**Lemma 2.8** (Normal form). Given  $a_1, \dots, a_{2^n} \in \mathbb{Z}$  and a skew  $2^n$ -gem computing the polynomial  $\prod_{i=1}^{2^n} (x - a_i)$ , there exist  $s \in \mathbb{Z}$  and  $t \in \{1, 2\}$  such that the polynomial  $\prod_{i=1}^{2^n} (x - t(a_i + s))$  is computed by a normalized  $2^n$ -gem.

*Proof.* In a skew circuit, if we have any addition gate with an input from another addition gate, we may replace both by one addition gate adding both constants to form one new constant, i.e.  $(x + a) + b = x(a + b)$ .

Since the degree of the polynomial computed by a gem has to double at each multiplication gate, such a gate must be of the form  $(y + a) * (y + b)$  with  $a, b \in \mathbb{Z}$ , where  $y$  is the output of the previous multiplication gate.

We can write  $(y + a) * (y + b) = y^2 + (a + b)y + ab$  as  $(y + (a + b)/2)^2 + ab - ((a + b)/2)^2$  and replace each multiplication gate accordingly. By combining sequential additions again, we get alternating  $\times$  gates and  $+$  gate; the  $+$  gate on the input level can be left out since it just shifts the zeros.

In case some  $(a + b)/2 \notin \mathbb{Z}$ , we can stretch the zeros by a factor of 2 by multiplying the constants on level  $i$  with  $2^{2^i}$ . ■

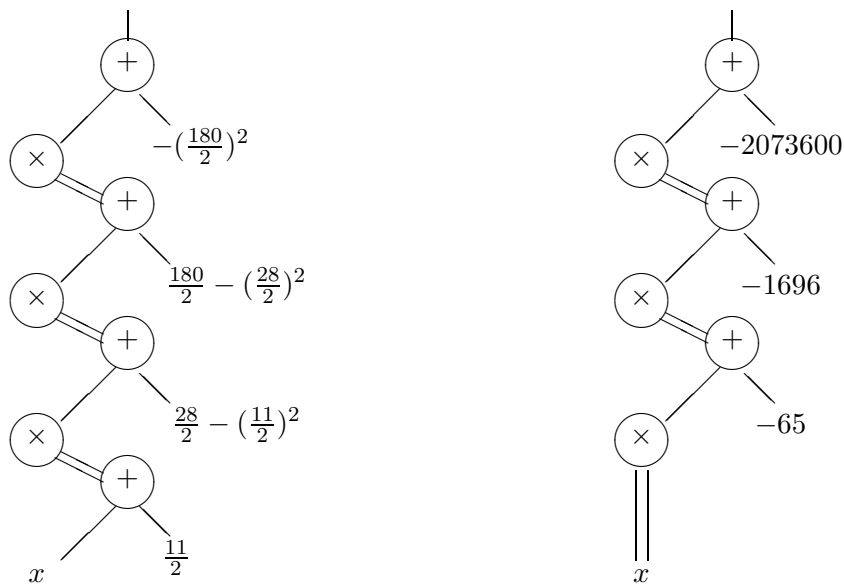


Figure 3: The example of the 8-gem from Figure 1 in alternating squaring form (left side) and after stretching by 2 (i.e.  $(-\frac{180}{2})^2 2^{16} = -2073600$ ) and shifting (right side).

An example of the transformation into normal form takes the 8-gem on the right of Figure 1 into the 8-gem depicted on the right of Figure 3.

**Proposition 2.10** (Well known, see [BoIn94].) The following are equivalent:

- $s_1 = t_1$  and  $s_2 = t_2$  and  $s_3 = t_3$  and  $\dots$  and  $s_k = t_k$
- $\text{degree}[p(x) - q(x)] \leq n - (k + 1)$ .

*Proof.* Apply Newton's formulas [Usp48] to  $p(x)$  and  $q(x)$ . These formulas relate the roots  $a_1, \dots, a_n$  of the polynomial  $p(x) = \sum_{i=0}^n c_k x^k$  to its coefficients by way of  $s_1, s_2, \dots, s_k$ :

$$\begin{aligned} s_1 + c_1 &= 0 \\ s_2 + c_1 s_1 + 2c_2 &= 0 \\ s_3 + c_1 s_2 + c_2 s_1 + 3c_3 &= 0 \\ &\vdots \\ s_n + c_1 s_{n-1} + c_2 s_{n-2} + \dots + n c_n &= 0. \end{aligned}$$

■

**Proposition 2.15.** Let  $A$  be  $\mathbb{Z}$ ,  $\mathbb{Q}$  or  $\mathbb{R}$ . Let  $p(x) \in \mathbb{R}[x]$  and  $q(x) \in \mathbb{R}[x]$ . If  $pq$  crumbles over  $A$  then both  $p$  and  $q$  crumble over  $A$ .

*Proof.* Let  $pq$  crumble over  $A$ . If  $\text{deg}(p) = \text{deg}(q) = 0$  then we are done. Otherwise, since  $\mathbb{R}$  is an entire ring, each root  $a \in A$  of  $pq$  satisfies  $p(a) = 0$  or  $q(a) = 0$ . The only way for  $p$  and  $q$  to account for the  $\text{deg}(p) + \text{deg}(q)$  distinct roots of  $pq$  in  $A$  is for  $p$  to absorb its maximum number  $\text{deg}(p)$  of such roots and for  $q$  to absorb the rest. Hence  $p$  and  $q$  crumble over  $A$ . ■

**Lemma 2.17.** Let  $e \in \mathbb{R}$  and suppose that a polynomial  $p(x) + e \in \mathbb{R}[x]$  of degree  $2^n$  crumbles over  $\mathbb{R}$ . Then the following holds:

**H1.** Any skew gem over  $\mathbb{R}$  for  $p(x)$  has at least  $n - 1$  additive gates.

**H2.** If  $e = 0$  then any skew gem over  $\mathbb{R}$  for  $p(x)$  has at least  $n$  additive gates.

*Proof.* We use induction on  $n$ . In the base case  $n = 0$ , there is nothing to prove. So let  $n \geq 1$  and consider any polynomial  $p(x) \in \mathbb{R}[x]$  of degree  $2^n$ . Let  $e \in \mathbb{R}$  be such that  $p + e$  crumbles. We need to prove that H1 and H2 hold for  $p(x)$ .

Consider any skew gem  $C$  over  $\mathbb{R}$  for  $p(x)$ . Being skew and having precisely  $n$  product gates,  $C$  has the tower form depicted on Figure 7 where each “ $\dots$ ” when present is a non-zero real constant. Let  $q(x) \in \mathbb{R}[x]$  be the polynomial computed by the subcircuit  $C_q$  rooted at the second  $\times$  gate nearest to the *output* of  $C$ , with  $q(x) = x$  when  $n = 1$ . Note that  $\deg(q) = 2^{n-1}$  and that  $C_q$  is a skew circuit having  $n - 1$  product gates. For some  $a, b, c \in \mathbb{R}$ ,  $p(x)$  is computed by  $C$  from  $q(x)$  as follows:

$$p(x) = (q(x) + a) \times (q(x) + b) + c.$$

Then

$$p + e = q^2 + (a + b)q + ab + c + e$$

and the derivative  $[p + e]'$  of  $p + e$  with respect to  $x$  satisfies

$$\begin{aligned} [p + e]' &= 2qq' + (a + b)q' \\ &= (2q + a + b)q' \\ &= [q + (a + b)/2] \cdot [2q']. \end{aligned}$$

By Rolle,  $[p + e]'$  crumbles. By Proposition 2.15,  $q + (a + b)/2$  crumbles. The inductive H1 therefore implies that  $C_q$  contains at least  $n - 2$  additive gates.

Proving H2 for  $p(x)$ :

We now assume that  $e = 0$ .

Case 1: Two or more among  $a$ ,  $b$  and  $c$  are nonzero. Then the total number of additive gates in  $C$  is at least  $2 + (n - 2) \geq n$ .

Case 2: Exactly one among  $a$ ,  $b$  and  $c$  is nonzero.

If  $c \neq 0$ , then  $q + (a + b)/2 = q$ . Then the inductive H2 implies that  $C_q$  has at least  $n - 1$  additive gates, for a total of at least  $1 + (n - 1) \geq n$  additive gates in  $C$ .

If  $c = 0$ , then assume with no loss of generality that  $a = 0$ . Since  $p + e = q(q + b)$  crumbles,  $q$  crumbles by Proposition 2.15. The inductive H2 again implies that  $C_q$  has at least  $n - 1$  additive gates, for a total of at least  $1 + (n - 1) \geq n$  additive gates in  $C$ .

Case 3:  $a = b = c = 0$ . Then  $p = q^2$  has repeated roots so this case is impossible.

Proving H1 for  $p(x)$ :

We now assume that  $e \neq 0$ .

We have just proved that H2 holds for any polynomial of degree  $2^n$ . Hence any gem over the reals for the crumbling degree- $2^n$  polynomial  $[p(x) + e] + 0$  requires at least  $n$  additive gates. It follows that any gem over the reals computing  $p(x)$  requires at least  $n - 1$  additive gates, as required.  $\blacksquare$

**Proposition 3.1:** For every  $d > 0$ , there exists an optimal  $d$ -gem over the reals.

*Proof.* Given a minimal addition chain  $a_1, \dots, a_{l_d}$  with  $a_{l_d} = d$ , we start with the input  $x$  as the gate of degree  $a_0 = 1$  and inductively define the subcircuit for degree  $a_i$  such that the function has  $a_i$  distinct zeros. For each  $i$  we consider the gates with degree  $a_j$  and  $a_k$  for  $j, k < i$  with  $a_i = a_j + a_k$ .

If the zeros of the corresponding functions are disjoint, we simply multiply the output of these gates and obtain a function with  $a_i$  distinct zeros.

If  $j = k$ , we also multiply (which means in this case we square) and obtain a function with  $a_k$  double zeros, then we subtract a constant  $\delta > 0$ , which is smaller than any local maximum of this function. This leads to  $a_i = 2a_k$  distinct zeros.

In the remaining case, we subtract a constant  $\delta > 0$ , which is smaller than any local maximum of the function from the gate of degree  $a_k$  and multiply with the gate of degree  $a_j$  and obtain a function with  $a_i$  distinct zeros.

In both cases, we can easily avoid the choice for  $\delta$  to result in one of the zeros to be identical with a zero that occurred before in the construction because there are only finitely such bad choices among infinitely many possible choices.  $\blacksquare$

**Theorem 3.4.** There exist 36-gems and 54-gems.

*Proof.* To get a 36-gem, we apply Lemma 3.3 with  $h(x) = (x^2 - 2s)^2$ , where  $s$  is a positive integer expressible in at least 9 essentially distinct ways as a sum of two nonzero squares (such numbers abound, see [Ro93, WIMS]):  $s = a_1^2 + b_1^2 = a_2^2 + b_2^2 = \dots = a_9^2 + b_9^2$ . Then we let  $m_i = 4s^2 - 16a_i^2b_i^2$  and observe that for each  $i$ ,

$$\begin{aligned} h(x) - m_i &= x^4 - 4sx^2 + 4s^2 - m_i \\ &= x^4 - 4(a_i^2 + b_i^2)x^2 + 16a_i^2b_i^2 \\ &= (x^2 - 4a_i^2)(x^2 - 4b_i^2) \\ &= (x + 2a_i)(x - 2a_i)(x + 2b_i)(x - 2b_i). \end{aligned}$$

Hence the 9 polynomials  $h(x) - m_i$  have pairwise disjoint sets of 4 distinct roots, and each has a gem by Lemma 3.2. Since  $\ell_4 + \ell_9 = 2 + 4 \leq \ell_{36} = 6$  and Lemma 3.2 also provides a 9-gem  $c_9$  such that  $f_{c_9}(y) = \prod_{i=1}^9 (y - m_i)$ , Lemma 3.3 yields a 36-gem for  $\prod_{i=1}^9 (h(x) - m_i)$ . To get a 54-gem, we apply Lemma 3.3 with  $h(x) = ((x^2 - s) \times x)^2$ , where  $s$  is a positive integer expressible in at least 9 essentially distinct ways in the form  $(a^2 + b^2 + ab)$ . Then we let  $m_i = (a_i b_i (a_i + b_i))^2$  and observe that for each  $i$ ,

$$\begin{aligned} h(x) - m_i &= ((x^2 - s) \times x)^2 - m_i \\ &= ((x^2 - (a_i^2 + b_i^2 + a_i b_i))x)^2 - (a_i b_i (a_i + b_i))^2 \\ &= ((x^2 - (a_i^2 + b_i^2 + a_i b_i))x - a_i b_i (a_i + b_i))((x^2 - (a_i^2 + b_i^2 + a_i b_i))x + a_i b_i (a_i + b_i)) \\ &= (x + a_i)(x + b_i)(x - a_i - b_i)(x - a_i)(x - b_i)(x + a_i + b_i). \end{aligned}$$

Hence the 9 polynomials  $h(x) - m_i$  have pairwise disjoint sets of 6 distinct roots, and each has a gem by Lemma 3.2. Since  $\ell_6 + \ell_9 = 3 + 4 \leq \ell_{54} = 7$  and Lemma 3.2 also provides a 9-gem  $c_9$  such that  $f_{c_9}(y) = \prod_{i=1}^9 (y - m_i)$ , Lemma 3.3 yields a 36-gem for  $\prod_{i=1}^9 (h(x) - m_i)$ . To get such an  $s$ , we apply the formula  $(a^2 + b^2 + ab)(c^2 + d^2 + cd) = (ac + bd + bc)^2 + (ad - bc)^2 + (ac + bd + bc)(ad - bc)$  instead of the Brahmagupta-Fibonacci equation iteratively in several combinations. For example  $7 = 2^2 + 1^2 + 2$  and  $13 = 3^2 + 1^2 + 3$  have this form thus  $((x^2 - 7)x)^2$  is 36 for  $x = -1, -2, 3, 1, 2, -3$ , the function  $((x^2 - 7 \cdot 13)x)^2$  is 90<sup>2</sup> for

$d$	$c_x$	$c_+$	$f_c(x)$	$\text{izeros}_c$
24	5		$f_{c_4}(y^2)$ with $y = (x^2 - 7 \cdot 13 \cdot 19)x$	$\{\pm 3, 40, 43, 8, 37, 45, 15, 32, 47, 23, 25, 48\}$
24	5	442	$z(z + c_{Prop.2.10})$ with $y = (x^2 - 11763)^2$ and $z = (y + 241x^2 + \dots)(y + 195x^2 + \dots)(y + x^2 + \dots)$	$\{\pm 22, 61, 86, 127, 140, 151, 35, 47, 94, 121, 146, 148\}$
25	6		The above $\times x$	The above $\cup \{0\}$
26	6	443	$f_{c_{24}} \cdot (x^2 - 1)$	$\text{Set}_{24} \cup \{-1, 1\}$
27	6		$y \times f_{c_4}(y^2)$ with $y = (x^2 - 7^2 \cdot 13^2)x$	$\text{Set}_{21} \cup \{\pm 49, 56, 105\}$
28	6	560	$f_{c_{24}} \cdot (y + 117x^2 + \dots)$	$\text{Set}_{24} \cup \{-1, 1, -153, 153\}$
29	7		The above $\times x$	The above $\cup \{0\}$
30	6		$f_{c_5}(y^2)$ with $y = (x^2 - 7^2 \cdot 13^2 \cdot 19)x$	$\{\pm 13, 390, 403, 35, 378, 413, 70, 357, 427, 103, 335, 438, 117, 325, 442\}$
31	7		The above $\times x$	The above $\cup \{0\}$
36	6		$f_{c_6}(y^2)$ with $y = (x^2 - 7^2 \cdot 13^2 \cdot 19)x$	$\text{Set}_{30} \cup \{\pm 137, 310, 447\}$
37	7		The above $\times x$	The above $\cup \{0\}$
42	7		$f_{c_7}(y^2)$ with $y = (x^2 - 7^2 \cdot 13^2 \cdot 19)x$	$\text{Set}_{36} \cup \{\pm 182, 273, 455\}$
54	7		$f_{c_9}(y^2)$ with $y = (x^2 - 7^2 \cdot 13^2 \cdot 19)x$	$\text{Set}_{42} \cup \{\pm 202, 255, 457, 225, 233, 458\}$
55	8		The above $\times x$	The above $\cup \{0\}$

Figure 4: Some  $d$ -gems as constructed for Theorem 3.4.

$x = -1, -9, 10, 1, 9, -10$  and  $330^2$  for  $x = -5, -6, 11, 5, 6, -11$ , the function  $(x^2 - 7 \cdot 7)x$  is 120 for  $x = -3, -5, 8$ , it is  $-120$  for  $x = 3, 5, -8$  and 0 for  $x = 0, -7, 7$ . The table

$x$ $((x^2 - 7 \cdot 13 \cdot 19)x)^2$	$\pm 3, 40, 43$ $m_1 = 5160^2$	$\pm 8, 37, 45$ $m_2 = 13320^2$	$\pm 15, 32, 47$ $m_3 = 22560^2$	$\pm 23, 25, 48$ $m_4 = 27600^2$	
$x$ $((x^2 - 7^2 \cdot 13^2 \cdot 19)x)^2$	$\pm 13, 390, 403$ $m_1 = 2043210^2$	$\pm 35, 378, 413$ $m_2 = 54663990^2$	$\pm 70, 357, 427$ $m_3 = 10670730^2$	$\pm 103, 335, 438$ $m_4 = 15113190^2$	$\pm 117, 325, 442$ $m_5 = 16807050^2$
$x$ $((x^2 - 7^2 \cdot 13^2 \cdot 19)x)^2$	$\pm 137, 310, 447$ $m_6 = 18984090^2$	$\pm 182, 273, 455$ $m_7 = 22607130^2$	$\pm 202, 255, 457$ $m_8 = 23540070^2$	$\pm 225, 233, 458$ $m_9 = 24010650^2$	

shows the values for constructing the gems in Figure 4. Note that the product  $7 \cdot 13 \cdot 19 \cdot 31$  respectively.  $7^2 \cdot 13 \cdot 19$  would already be sufficient for the construction of a 42-gem respectively. 36-gem and produce smaller numbers there.  $\blacksquare$

Multiplying our 54-gem with  $(x - a_{55})$  leads to the 55-gem  $f_{c_9}(h(x)) \cdot (x - z_{55})$  which is the highest which we found.

PTE solutions are useful for an alternative construction of a 24-gem in Figure 4. Indeed, if we don't care about the number of additive gates, we can assume that any constant multiple of  $x^2$  is available once  $x^2$  is. We use the symmetric ideal solution  $\{22, 61, 86, 127, 140, 151\}$ ,  $\{35, 47, 94, 121, 146, 148\}$  found by Kuosa, Meyrignac and Shuwen [Shu01] to construct a circuit with 5 multiplications and 24 zeros as follows. Note that the polynomial

$$p(x) = (x^2 - 22^2)(x^2 - 61^2)(x^2 - 86^2)(x^2 - 127^2)(x^2 - 140^2)(x^2 - 151^2)$$

can be computed using 4 products, for example by calculating  $x^2$  and  $(x^2 - 11763)^2 = x^4 - 23526x^2 + 11763^2$  using 2 multiplications, then calculating  $(x^4 - 23285x^2 + 22^2 \cdot 151^2)$ ,  $(x^4 - 23321x^2 + 61^2 \cdot 140^2)$  and  $(x^4 - 23525x^2 + 86^2 \cdot 127^2)$  using (only a few hundred) additions, and finally computing  $p(x)$  by multiplying the latter three polynomials using 2 more products. By Proposition 2.10, there exists a constant  $c_{Prop2.10} \in \mathbb{Z}$  such that

$$p(x) + c_{Prop2.10} = (x^2 - 35^2)(x^2 - 47^2)(x^2 - 94^2)(x^2 - 121^2)(x^2 - 146^2)(x^2 - 148^2),$$

Hence one last product computes the 24-gems  $p(x) \times (p(x) + c_{Prop2.10})$ .

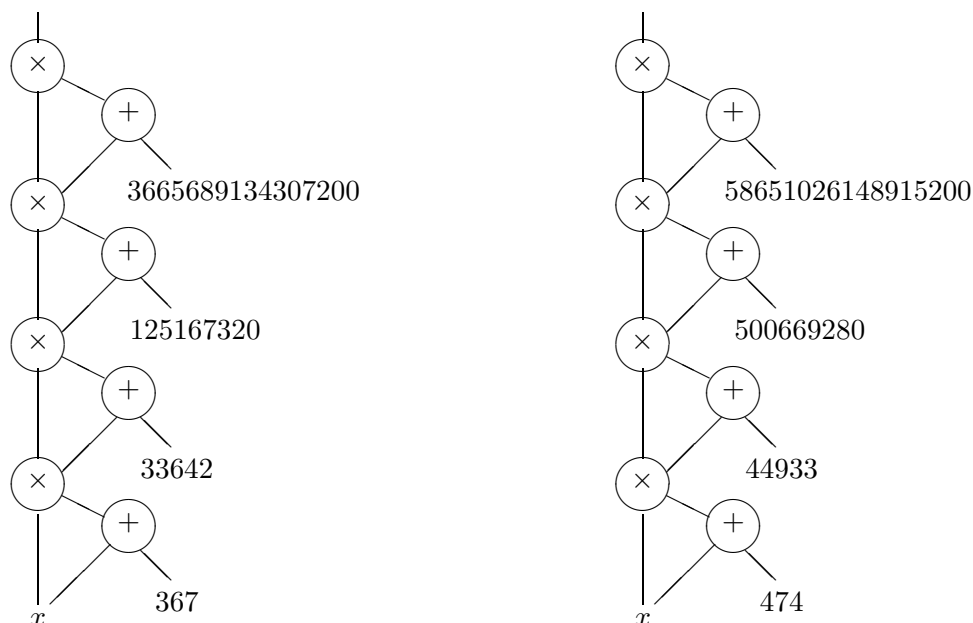


Figure 5: Two 16-gems, found by a Java applet running several hours on a PC.

## 5. $d$ -gems when $d$ is a power of 2: (redundant but more explicit version of Section 2)

We are interested in arithmetic circuits with many different integer zeros but only few gates. The arithmetic circuit shown in the middle of Figure 1 has 6 gates and 8 different integer zeros:  $0, -1, -2, -4, -7, -9, -10, -11$ . This can be checked by brute force. The circuit already has fewer gates than zeros. We can improve on this ratio. The arithmetic circuit shown on the left of Figure 5 has 8 gates and 16 different integer zeros:

$0, -4, -7, -12, -118, -133, -145, -178, -189, -222, -234, -249, -355, -360, -363, -367$ .

This can again be verified by computing the values  $f_c(0), f_c(-4), \dots, f_c(-367)$  which are all 0. As another example, the circuit shown on the right of Figure 5 also has 16 different zeros:

$0, -19, -10, -48, -59, -96, -111, -131, -343, -363, -378, -415, -426, -455, -464, -474$ .

### 5.1. A systematic construction for 8-gems

We will show how to construct an 8-gem from any pair of prime numbers congruent to 1 modulo 4.

It is well known that any prime congruent to 1 modulo 4 can be written as a sum of two squares. Using Proposition 2.4, distinct integers  $a, b, c$  and  $d$  satisfying (E8.1) are thus easy to come by. For example, with  $p = 5 = 1^2 + 2^2$  and  $q = 13 = 2^2 + 3^2$  we get  $a = 8, b = 1, c = 4, d = 7$  satisfying  $8^2 + 1^2 = 4^2 + 7^2$ .

Now let there be given four different integers  $a, b, c, d > 0$  such that  $a^2 + b^2 = c^2 + d^2$ . Consider the arithmetic circuit shown on the left of Figure 6. Obviously,  $a$  and  $-a$  are zeros of the circuit because they make the lowest multiplication gate 0. Also  $b$  is a zero of the circuit because  $(b - a)(b + a) = b^2 - a^2$ , and therefore the second lowest multiplication gate

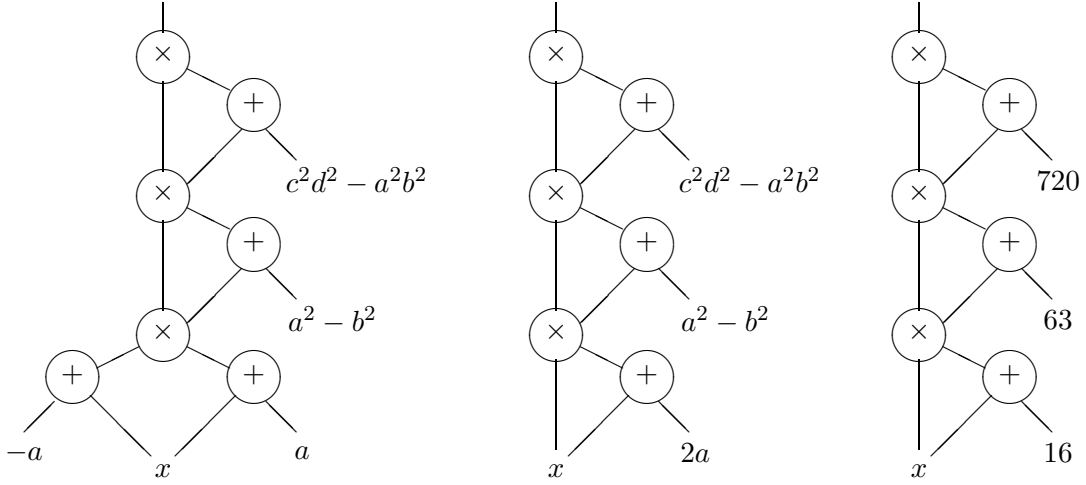


Figure 6: An 8-gem, given the equation  $a^2 + b^2 = c^2 + d^2$ .

will have the value 0, likewise this holds for  $-b$ . If the input  $x$  is set to  $c$  or  $-c$ , then the highest addition gate will have the value

$$\begin{aligned} (c+a)(c-a)((c+a)(c-a) + a^2 - b^2) + c^2d^2 - a^2b^2 &= (c^2 - a^2)(c^2 - b^2) + c^2d^2 - a^2b^2 \\ &= c^4 - c^2(a^2 + b^2) + a^2b^2 + c^2d^2 - a^2b^2 = c^4 - c^2(a^2 + b^2) + c^2d^2 \\ &= c^4 - c^2(c^2 + d^2) + c^2d^2 = (c^2 - c^2)(c^2 - d^2) = 0. \end{aligned}$$

For the same reason, also  $d$  and  $-d$  are zeros of the circuit. Summarizing, the circuit has the zeros  $a, -a, b, -b, c, -c, d, -d$ . It still has four addition gates. By a linear transformation  $x \rightarrow x + a$  we obtain the 8-gem shown in the center of Figure 6, having the eight zeros

$$0, -2a, b - a, -b - a, c - a, -c - a, d - a, -d - a.$$

The circuit on the right of Figure 6 is obtained by using  $a = 8, b = 1, c = 4, d = 7$ ; its zeros are:  $0, -16, -7, -9, -4, -12, -1, -15$ , as can be double-checked by evaluation.

## 5.2. Constructing 16-gems

The previous construction can be extended to a construction for 16-gems, and possibly for  $2^n$ -gems. We assume that we are given 8 different integers  $a, b, c, d, e, f, g, h > 0$  such that the following 4 equations hold:

$$a^2 + b^2 = c^2 + d^2 = e^2 + f^2 = g^2 + h^2, \quad (\text{E16.1} - \text{E16.3})$$

$$(ab)^2 + (cd)^2 = (ef)^2 + (gh)^2. \quad (\text{E16.4})$$

Consider the circuit shown on the left of Figure 9. We show that under the assumptions this is a 16-gem. For the same reasons as for the circuit in the center of Figure 6 it has the zeros  $0, -2a, b - a, -b - a, c - a, -c - a, d - a, -d - a$ , in other words, the value at the second highest multiplication gate is

$$((x+a)^2 - a^2)((x+a)^2 - b^2)((x+a)^2 - c^2)((x+a)^2 - d^2).$$

Therefore, the value for  $x = e - a$  at the highest addition gate is

$$\begin{aligned}
& (e^2 - a^2)(e^2 - b^2)(e^2 - c^2)(e^2 - d^2) + (efgh)^2 - (abcd)^2 \\
&= (e^4 - e^2(a^2 + b^2) + a^2b^2)(e^4 - e^2(c^2 + d^2) + c^2d^2) + (efgh)^2 - (abcd)^2 \\
&= (e^4 - e^2(a^2 + b^2) + a^2b^2)(e^4 - e^2(a^2 + b^2) + c^2d^2) + (efgh)^2 - (abcd)^2 \\
&= (e^4 - e^2(a^2 + b^2))^2 + (e^4 - e^2(a^2 + b^2))(a^2b^2 + c^2d^2) + a^2b^2c^2d^2 + (efgh)^2 - (abcd)^2 \\
&= (e^4 - e^2(e^2 + f^2))^2 + (e^4 - e^2(g^2 + h^2))(e^2f^2 + g^2h^2) + (efgh)^2 \\
&= (e^4 - e^2(e^2 + f^2) + e^2f^2)(e^4 - e^2(g^2 + h^2) + g^2h^2) \\
&= (e^2 - e^2)(e^2 - f^2)(e^2 - g^2)(e^2 - h^2) = 0.
\end{aligned}$$

Likewise, the values for  $x = -e - a$ ,  $x = f - a$ ,  $x = -f - a$ ,  $x = g - a$ ,  $x = -g - a$ ,  $x = h - a$ ,  $x = -h - a$  at the highest addition gate are 0. Therefore, the circuit shown on the left of Figure 9 is a 16-gem, given the equations (E16.1-4) do hold. As an example, for the values

$$a = 237, b = 106, c = 189, d = 178, e = 227, f = 127, g = 218, h = 141$$

the equations (E16.1-4) hold, as can be checked by evaluation. The circuit constructed as above is the one shown on the right of Figure 5.

### 5.3. Constructing 32-gems and beyond

What follows now is a hypothetical construction, in the sense that the authors do not know whether the assumption can be fulfilled. We assume that we are given 16 different integers  $a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p > 0$  such that the following 11 equations hold:

$$a^2 + b^2 = c^2 + d^2 = e^2 + f^2 = g^2 + h^2 = i^2 + j^2 = k^2 + l^2 = m^2 + n^2 = o^2 + p^2, \quad (\text{E32.1} - \text{E32.7})$$

$$(ab)^2 + (cd)^2 = (ef)^2 + (gh)^2 = (ij)^2 + (kl)^2 = (mn)^2 + (op)^2, \quad (\text{E32.8} - \text{E32.10})$$

$$(abcd)^2 + (efgh)^2 = (ijkl)^2 + (mnop)^2. \quad (\text{E32.11})$$

Then the circuit shown on the right of Figure 9 is a 32-gem, as can be shown by the methods from above.

This leads to a general construction for  $2^n$ -gems, under the hypothesis that a set of integers exists with the required properties. Assume that there are  $2^n$  different integers  $a_1, \dots, a_{2^n} > 0$  such that the following equations hold:

$$a_1^2 + a_2^2 = a_3^2 + a_4^2 = \dots = a_{2^{n-1}}^2 + a_{2^n}^2, \quad (\text{E}2^{n+1}.1 - \text{E}2^{n+1}.2^{n-2} - 1)$$

$$(a_1a_2)^2 + (a_3a_4)^2 = \dots = (a_{2^{n-3}}a_{2^{n-2}})^2 + (a_{2^{n-1}}a_{2^n})^2, \quad (\text{E}2^{n+1}.2^{n-2} - \text{E}2^n.2^{n-2} + 2^{n-3} - 2)$$

...

$$(a_1 \dots a_{2^{n-2}})^2 + (a_{2^{n-2+1}} \dots a_{2^{n-1}})^2$$

$$= (a_{2^{n-1+1}} \dots a_{2^{n-1+2^{n-2}}})^2 + (a_{2^{n-1+2^{n-2}+1}} \dots a_{2^n})^2. \quad (\text{E}2^{n+1}.2^{n-1} - n - 1)$$

Then one can construct a  $2^{n+1}$ -gem.

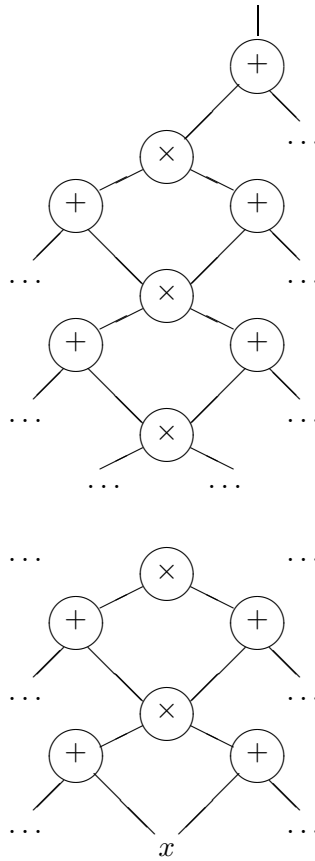


Figure 7: The "tower" structure of a  $2^m$ -gem (in case it exists)

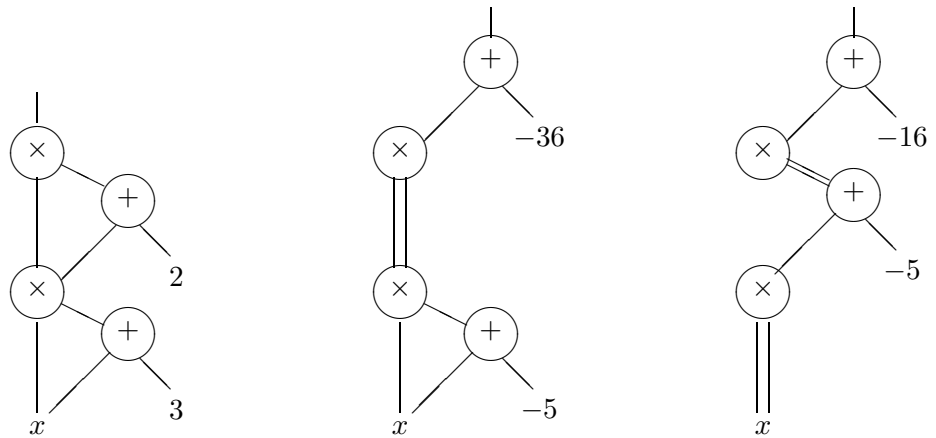


Figure 8: Different shapes of 4-gems. The middle gem computes the function  $(x \cdot (x - 5))2 - 36$  having zeros at  $-1, 2, 3, 6$ , showing that two product gates need not be separated by an additive gate.

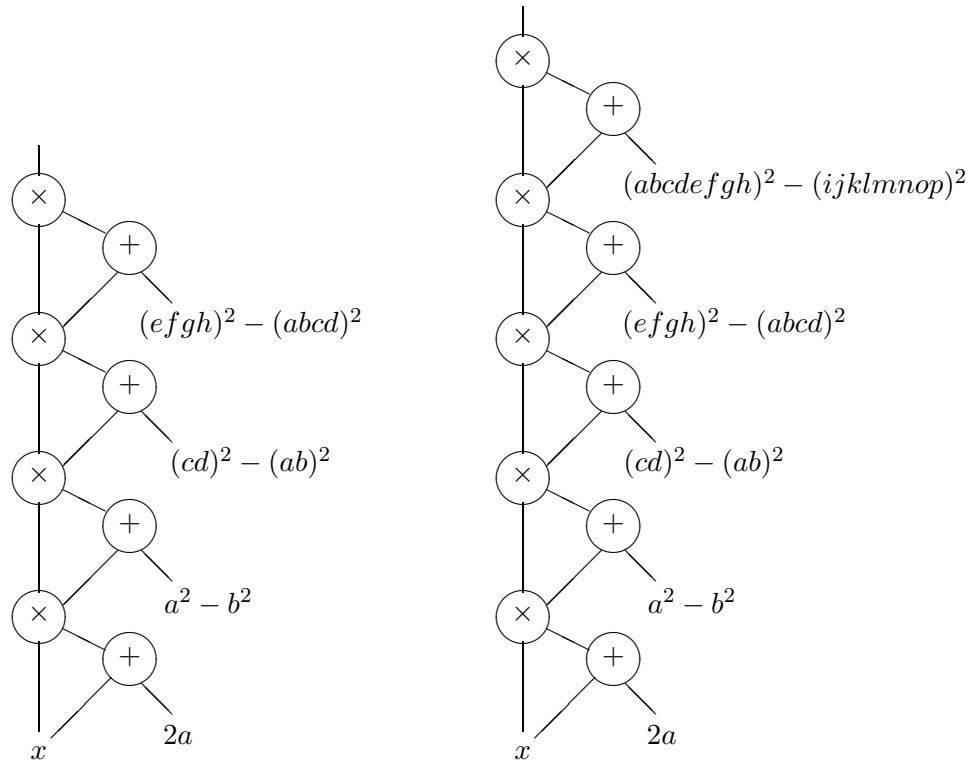


Figure 9: A 16-gem and a hypothetical 32-gem, assuming specific relationships among the parameters.

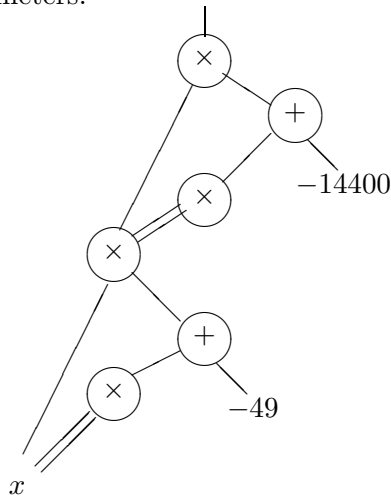


Figure 10: The 9-gems from our table listing all our  $d$ -gems. It has only 6 gates in total and its zeros are  $-8, -7, -5, -3, 0, 3, 5, 7, 8$ . This shows that a circuit with  $2n$  gates can have more than  $2^n$  distinct integer zeros.