On the Complete Base Polynomials — A high school student's story of math research

Alex Chen
York High School & Stanford University

1 My Research Experience

Involving high school students in research has been a long standing practice in the experimental sciences. However, it has only been recently that high school students have been involved in mathematics research in significant numbers. The realm of mathematics is in many ways both the most and least accessible field to conduct research. Mathematics requires none of the complex and expensive lab equipment or test specimens required to do work in many other fields. For most mathematics research, all is needed are pencil, paper, computer, and a hearty interest and determination. But, on the other hand, most interesting mathematics problems are often very inaccessible to students with a high-school math background. To comprehend the problems, a great deal of independent study in the background material is often needed. Thus, achieving success in mathematics research lies in the selection of appropriate problems. An ideal problem should not require much background reading, have probable partial results are probable, and have new results that are likely publishable. Regarding the limited math background of a high school student, a math mentor is invaluable in providing perspective on potential problems, having the experience to understand which problems seem more accessible. A mentor is also important in being able to know what types of background knowledge are necessary to understand the problems, so that the student can spend less time trying to understand the problem and more time actually solving it.

I was one of about 75 extremely lucky students from around the world selected to attend the Research Science Institute (RSI) last summer. The RSI is an intensive 6-week summer program for rising high school seniors held at the Massachusetts Institute of Technology, where

students are guided by professors, graduate students, and researchers in the Boston area. In addition to the wonderful research opportunities, one of the greatest benefits of participating in the RSI lies in the interaction with the other brilliant high school students. About a third of the students attending are international, hailing from countries such as Bulgaria, China, Germany, Saudi Arabia and Singapore. I came away from the RSI having made a number of wonderful friends, many of whom I have no doubt will be among the big names in science in the near future.

Mr. Brian Lehmann, a graduate student in the MIT Mathematics Department, served as my mentor at RSI. He proposed a number of problems to me, and we spent a few days debating the merits of choosing to work on each. I eventually decided on a number theory problem regarding complete base polynomials, which are the extension of the concept of integer bases to the polynomials. Further information regarding my research is detailed in section 2.

After deciding on a research topic, I realized that I understood very little of the underlying mathematical machinery behind the proofs previously made on the topic. For nearly an entire week, I spent many hours a day in MIT's Hayden Library, immersing myself in introductory books on number theory and abstract algebra. It was a near-overwhelming amount of new notations, concepts, and ideas to absorb in such a short period of time, but I enjoyed the challenge and enthusiastically threw myself into mastering the mathematics necessary to solve my problem. In that short period of time, I learned the basics of group theory, radix representations, and residue classes, just to name a few.

Once equipped with this new knowledge and feeling confident enough to begin work on my problem, I was left with approximately four weeks for research. I spent much of the time working in computer labs or in quiet classrooms, solving the case analysis and theorems needed to complete my proof. I also heavily relied on the Mathematica computer program, eventually writing my own code that allowed me to test specific examples, which proved to be extremely useful in my research. Throughout this entire process, my mentor gave me helpful suggestions on how to clearly express my work in a paper and how to systematically analyze overwhelming quantities of cases. However, as was true with many of my peers also doing math research, the entire experience was very independent, and I had a significant amount of freedom to decide when, where, and how I wanted to work. Near the end of the RSI, I was able to complete the proof that I had set out as my goal for the program.

Although I had reached the results that I wanted, the entire concept of base polynomials and its applications greatly intrigued me and I continued to study them once RSI had ended and I returned home. No longer having MIT's considerable resources at my disposal, I relied more on email correspondences with leading researchers in my field to help me decide on directions for further study. In the month following the RSI, I managed to isolate a number of important counterexamples as well as formulated several conjectures regarding the behavior of more complex base polynomials.

The RSI gave me an invaluable opportunity to conduct independent research. I felt that, though the experience was highly abbreviated, it was one of the most eye-opening 6 weeks of my life, and greatly reinforced and narrowed my passions for mathematics and science. My research experience taught me that dedication, commitment, and passion are necessary to achieve the results that you want. No one wants to be working on a problem that they don't truly enjoy, so finding a topic in a field which you can be passionate about is essential to having both enjoyable and productive research.

I was extremely fortunate that my research actually managed to produce substantial results in the brief weeks I spent at RSI. However, I am much more thankful that I had the chance to taste what an actual research experience is like, rather than the fact that I created an end product. I am certainly proud of what I achieved, but the learning experience itself was far more valuable to me than any awards won.

2 My Research Paper

My paper is entitled "On the Reducible Quintic Complete Base Polynomials." The background and main results with brief, summarized proofs are given as follows and the full version is available from the author. Hopefully this piece will inspire other interested high school students to cast away their reservations and pursue their own independent research.

2.1 Introduction

It is well known that every $n \in \mathbb{N}$ can be expressed uniquely as

$$n = c_0 + c_1 b + \cdots + c_m b^m,$$

where the integer base, or radix, $b \geq 2$, the coefficient $c_m \neq 0$, and $c_i \in \{0, 1, 2, \cdots, b-1\}$. This concept has been generalized to different bases and numeration systems.

Grunwald [7] studied the negative bases, and in particular showed that every $n \in \mathbb{Z}$ admits a unique representation

$$n = d_0 + d_1(-b) + \cdots + d_\ell(-b)^\ell,$$

where the base $b \geq 2$, the coefficient $d_\ell \neq 0$ and $d_i \in \{0, 1, 2, \cdots, b-1\}$. A famous example that used negative bases is the negadecimal system.

Knuth [9] observed that the Gaussian integers $\mathbb{Z}[i]$ admit a unique representation with radix $b = -1 + i$. In last decade, these concepts have been further extended to the following generalized base representations.

Definition. Let

$$B(x) = x^m + b_{m-1}x^{m-1} + \cdots + b_0 \in \mathbb{Z}[x] \tag{1}$$

and $S = \{0, 1, 2, \cdots, |b_0| - 1\}$. If every $P(x) \in \mathbb{Z}[x]$ has an expression of the form

$$P \equiv Q \pmod{B},$$

where $Q(x) \in \mathbb{Z}[x]$ has all coefficients in S, then we say that (B, S) is a complete base (CB) or canonical number system (CNS). In the sequel we use the term complete base (CB) and refer to $B(x)$ as a CB polynomial.

Not all polynomials $B(x)$ will form a complete base. It is easy to show that $B(x) = x + b_0$ with $b_0 \geq 2$ forms a complete base. For the quadratic polynomials $B(x) = x^2 + b_1x + b_0$, Gilbert [6] proved that B is a CB polynomial if and only if $-1 \leq b_1 \leq b_0$ and $b_0 \geq 2$. It is natural to ask whether there exists a complete classification of all CB polynomials. Unfortunately, existing research results indicate that the structure of CB polynomials (even polynomials of only degree three) is very complicated and only partial results have been achieved. Recently, Kane [8] found a class of CB polynomials which have k distinct integer roots with $k \leq 4$.

The purpose of this paper is to characterize completely reducible quintic CB polynomials. Our results extend Kane's recent work to $k = 5$. We also provide a Mathematica program that determines whether a given polynomial $B(x)$ is a CB polynomial or not.

2.2 Preliminaries

In this section, we review some existing results regarding CB polynomials.

Theorem 1 (Pethö [11], Kane [8]). *If $B(x)$ is a CB polynomial, then*

1. *all roots of $B(x)$ lie outside the closed unit disk, and*
2. *all real roots of $B(x)$ are less than -1.*

The linear and quadratic CB polynomials are completely determined by the comparative sizes of their coefficients. Thus, we are interested in generally characterizing CB polynomials by the sizes of their coefficients.

There are three special cases that necessitate our attention. The first describes the "monotonicity condition" on the coefficients of CB polynomials.

Theorem 2 (Pethö [10]). *If $B(x)$ has no roots on the closed unit disk and its coefficients satisfy*

$$b_0 \geq 2 \text{ and } b_0 \geq b_1 \geq \cdots \geq b_{m-1} > 0,$$

then B is a CB polynomial.

The second theorem describes the "dominance condition" on the coefficients of CB polynomials.

Theorem 3 (Akiyama and Pethö [3]). *If $B(x)$ has no roots on the closed unit disk and its coefficients satisfy*

$$b_2, \ldots, b_{m-1} \geq 0, \sum_{k=1}^{m} b_k \geq 0 \text{ and } b_0 > \sum_{k=1}^{m} |b_k|,$$

then B is a CB polynomial.

The third result characterizes completely reducible polynomials of degree four and below.

Theorem 4 (Pethö [10], Kane [8]). *If B is a polynomial whose roots are k distinct integers less than -1, if $k \leq 4$, and $S = \{0, 1, \ldots, b_0 - 1\}$, then (B, S) forms a complete base.*

Unfortunately, few results exist for $k \geq 5$. Kane [8] provides a counterexample for $k = 9$, showing that the analogue of Theorem 4 does not hold for arbitrary k.

2.3 The characterization of quintic complete base polynomials

In this section we extend Theorem 4 to completely reducible quintic polynomials. The following theorem provides an alternate requirement for (B, S) forming a complete base.

Theorem 5 (Kane [8]). *(B, S) forms a complete base if and only if B has no roots on the closed unit disk and there exists no polynomial $T \in \mathbb{Z}[x]$ and natural number n so that when $B \cdot T$ is reduced modulo $1-x^n$ to a polynomial of degree at most $n-1$ it is a nonzero polynomial with coefficients in S.*

For any given B that satisfies the two conditions of Theorem 1, the maximum and minimum bounds for the coefficients of T are determined as follows

Lemma 6 (Kane [8]). *If B has only negative integer roots other than -1 and $T \in \mathbb{Z}[x]$ has degree less than n so that $B(x)T(x) \equiv U(x) \pmod{1-x^n}$ where $U(x)$ has degree less than n and coefficients in $\{0, 1, \ldots, b-1\}$, then all of the coefficients of T are in the interval*

$$\left[\frac{b-1}{2}\left(-\frac{1}{B(-1)}+\frac{1}{B(1)}\right), \frac{b-1}{2}\left(\frac{1}{B(-1)}+\frac{1}{B(1)}\right)\right].$$

In particular, for the quintic case, we have

Corollary 7. *If*

$$B(x) = (x+\alpha)(x+\beta)(x+\gamma)(x+\delta)(x+\epsilon) = x^5 + p_1x^4 + p_2x^3 + p_3x^2 + p_4x + p_5, \qquad (2)$$

where $\alpha, \beta, \gamma, \delta, \epsilon$ are distinct integers greater than or equal to 2, then the coefficients of T are in the set $\{-2, -1, 0, 1, 2, 3\}$.

We are now in the position to characterize completely reducible quintic CB polynomials.

Theorem 8. *If B is a polynomial given by (2) whose roots are five distinct integers less than -1, and $S = \{0, 1, \ldots, p_5 - 1\}$, then (B, S) forms a complete base.*

The following lemma provides considerable machinery to prove Theorem 8.

Lemma 9. *If $B(x)$ is a polynomial given by (2) whose roots are five distinct integers less than -1, then the following inequalities hold:*

1. $2p_5 + p_4 > 3p_3 + 3p_2 + 3p_1 + 3$,
2. $p_5 + 2p_4 > 3p_3 + 3p_2 + 3p_1 + 3$,
3. $2p_5 + p_3 > p_4 + 3p_2 + 3p_1 + 3$,
4. $2p_5 > p_3 + 3p_2 + 3p_1 + 3$,
5. $p_5 + p_4 > 2p_3 + 3p_2 + 3p_1 + 3$,
6. $p_4 > p_3 + 2p_2 + 2p_1 + 2$,
7. $p_5 > 2p_2 + 2p_1 + 2$,
8. $p_5 > p_3 + 3p_1 + 3$,
9. $2p_5 > p_4 + 2p_2 + 3p_1 + 3$,
10. $p_5 + p_4 + p_2 > 3p_3 + 3p_1 + 3$,
11. $2p_5 + 2p_2 > 3p_3 + 3p_1$,
12. $p_4 + p_2 + 2 > 2p_3 + 2p_1$
13. $p_3 > 2p_2 + 2p_1 + 2$,
14. $p_5 + p_3 > p_4 + p_2 + 2p_1 + 1$,
15. $p_5 + 2p_3 + p_1 > p_4 + 2p_2 + 2$,
16. $2p_4 > 3p_3 + 4$,
17. $2p_4 + 3p_2 > 4p_3 + 4p_1 + 4$,
18. $p_2 > 2p_1 + 1$,
19. $p_1 > 2$.

The proof is based on the following well-known fact regarding symmetric functions:

Proposition 10. *Let $f(x_1, x_2, \ldots, x_n)$ be symmetric, i.e.,*

$$f(x_1, x_2, \ldots, x_n) = f(\sigma(x_1, x_2, \ldots, x_n)),$$

where $\sigma(x_1, x_2, \ldots, x_n)$ is a permutation of $(x_1, x_2, \ldots, x_n)$. If f is continuous and increasing for each x_i in $a_i \leq x_i < \infty$, then

$$f(x_1, x_2, \ldots, x_n) \geq f(a_1, a_2, \ldots, a_n).$$

Now, we turn to the proof of Theorem 8.

Proof of Theorem 8. Suppose for the sake of contradiction that (B, S) does not form a complete base. Since B has no roots on the closed unit disk, by Theorem 5, we just have to prove that there exists no polynomial $T \in \mathbb{Z}[x]$ of degree less than n so that when $B \cdot T$ is reduced modulo $1 - x^n$ the result has coefficients in S. Suppose that such a T does exist. Let

$$T(x) = t_0 + t_1 x + t_2 x^2 + \cdots + t_{n-1} x^{n-1} \tag{3}$$

and

$$B \cdot T = s_0 + s_1 x + \cdots + s_{n-1} x^{n-1} + (1 - x^n) q(x), \tag{4}$$

where $s_i \in S$ for all $0 \leq i \leq n - 1$ and

$$q(x) = q_0 + q_1 x + q_2 x^2 + q_3 x^3 + q_4 x^4.$$

Then, in general, for $0 \leq k \leq n - 1$, we have

$$s_k = p_5 t_k + p_4 t_{k-1} + \cdots + p_1 t_{k-4} + t_{k-5}, \tag{5}$$

where the indices of the t_i are taken modulo n.

We now show that for any given polynomial T, at least one of the coefficients of (5) is either negative or greater than $p_5 - 1$. This contradicts to the assumption that $s_k \in S$.

First, we demonstrate that *thirty cases* of coefficient strings cannot appear in T for the given reasons, which imply the full cases.

Next, we explicitly analyze and prove the nonexistence of one typical coefficient strings: Case 1 $(-2/(-1), -2)$. The derivations of rest cases are analogous.

For Case 1, the possible coefficients for the x^k term of $B \cdot T$ would be

$$-2p_5 - 2p_4 + ap_3 + bp_2 + cp_1 + d \quad \text{or} \quad -2p_5 - p_4 + ap_3 + bp_2 + cp_1 + d.$$

These two terms are achieved by $t_k = -2, t_{k-1} = -2/(-1)$. To verify that the coefficient string $(-2/(-1), -2)$ cannot appear in a T as in Theorem 5, we show that both of these coefficients in $B \cdot T$ are negative. We only address

$$-2p_5 - p_4 + ap_3 + bp_2 + cp_1 + d < 0 \tag{6}$$

because confirming (6) immediately implies both terms to be negative and disproves both $(-2, -2)$ and $(-1, -2)$.

It is easy to see that (6) is equivalent to

$$2p_5 + p_4 > ap_3 + bp_2 + cp_1 + d,$$

and by Corollary 7, $a, b, c, d \in \{-2, -1, 0, 1, 2, 3\}$. Thus the right hand side of the inequality is maximized when $a, b, c, d = 3$ and (6) is valid by Lemma 9.1. □

2.4 A Complete Base polynomial test program

In this section we introduce a Mathematica program which determines whether a given polynomial $B(x)$ is a CB polynomial or not.

The principle of this program is based on Brunotte's mapping. Define $\tau : \mathbb{Z}^m \to \mathbb{Z}^m$ by

$$\tau(x_1, x_2, \cdots, x_m) = \left(-\text{sign}(b_0) \lfloor \frac{\sum_{i=1}^{m} b_i x_i}{b_0} \rfloor, x_1, x_2, \cdots, x_{m-1} \right).$$

Brunotte [5] proved that

Theorem 11. *If $E \subseteq \mathbb{Z}^m$ has the following properties:*

- $(1, 0, \ldots, 0) \in E$,

- $-E \subseteq E$,
- $\tau(E) \subseteq E$,
- *For every* $x \in E$ *there exists some* $k \in \mathbb{N}$ *such that* $\tau^k(x) = 0$.

then B *is a CB polynomial.*

Theorem 11 provides the following algorithmic process to test whether $B(x)$ is a CB polynomial or not.

1. Begin with $E_1 = \{(0, 0, \ldots, 0), (-1, 0, \ldots, 0), (1, 0, \ldots, 0)\}$,
2. If E_i is defined for $i < k$ then E_k is defined by $E_k = E_{k-1} \cup \tau(E_{k-1}) \cup (-\tau(-E_{k-1}))$,
3. If $E_k \neq E_{k-1}$ then repeat step (2), otherwise go to step (4),
4. For each $x \in E_k$, confirm that there exists some $l \in \mathbb{N}$ such that $\tau^l(x) = 0$.

Note that $E_k = -E_k$ for all k. If $B(x)$ has no roots on the closed unit disk, step (4) will terminate in a finite number of steps. In addition, because τ is eventually contractive, the set $E_k(k = 1, 2, \ldots)$ must be uniformly bounded. By the discreteness of $\mathbb{Z}^m$ in $\mathbb{R}^m$ and $E_k \supset E_{k-1}$, step (2) will also terminate in a finite number of steps.

Implementing this algorithm in Mathematica, we establish a CB polynomial test program (See Appendix for code), which enables us to experiment with higher degrees of polynomials, to decide if the potential result points in the desired direction and to formulate credible conjectures. By using this program, we have the following interesting observations.

1. Theorem 8 does not hold for quintic polynomials with non-real roots. For example, $(x + 2)(x^2 - 2x + 2)(x^2 - x + 3)$ and $(x + 2)(x + 3)(x + 4)(x^2 - 2x + 2)$ are not CB polynomials. Thus, the completely reducible condition in Theorem 8 is necessary.
2. It is well known that the product of a linear and a quadratic CB polynomial is a CB polynomial. However, this no longer holds for higher degree polynomials. For example, the product of both CB polynomials $x^2 - x + 2$ and $x^2 - x + 3$ is no longer a CB polynomial. In quintic cases, the counterexample is given by the CB polynomial pair $x^3 + 80x^2 + 117x + 89$ and $x^2 - x + 2$.
3. If $B(x) = \prod_{i=2}^{n}(x + i)$, then $n = 10$ yields Kane's [8] counterexample. The program shows that $B(x)$ is not a CB polynomial for $10 \leq n \leq 16$, however, $B(x) = \prod_{i=3}^{11}(x + i)$ is a CB polynomial.

4. Let $B(x) = \prod_{i=1}^{n} (x + r_i)$ with $r_i \geq 2$. For sufficient large roots, for example,

$$\sum_{i=1}^{n} \frac{1}{r_i} \leq 1 \tag{7}$$

the program shows that $B(x)$ is a CB polynomial. In light of those results, in general, we conjecture that $B(x)$ is a CB polynomial if (7) holds. Surprisingly, Newton's inequalities for symmetric functions show that (7) implies Pethö's monotonicity condition in Theorem 3 and so yields a rigorous proof of this conjecture. We will address the details in a forthcoming paper.

2.5 Concluding remarks

We have characterized the completely reducible quintic CB polynomials. This is the best possible result regarding the completely reducible polynomials so far. Theoretically, by using the same argument, one could analyze equivalent assertions for $k \geq 6$. However, this would widen the range of possible coefficients of polynomial T as dictated by Lemma 6, greatly increasing the number of coefficient strings which must be examined. Meanwhile, our CB polynomial test program yields that the analogue of Theorem 4 fails for $k \geq 9$ in general. At this point, there is no method that is guaranteed to succeed in characterizing complete reducible CB polynomials of kth degree with $6 \leq k < 9$, and new ideas are required.

Appendix

Complete base polynomial test program code in Mathematica

```
P1 = [INSERT B(X) HERE];
LP = CoefficientList[P1, x];
Print[Pl];
Clear[L1];
r = x /. NSolve[P1 == 0, x];
Print[r];
For[i = 1, i <= Length[r], i++, If [Abs[Part[r, i]] < = 1,
Print[‘‘Root on Closed Unit Disk’’];
Abort[]];];
C1 = Drop[CoefficientList[P1, x], 1];
L ={-First[IdentityMatrix[Length[C1]]],
-Last[IdentityMatrix[Length[C1]]],
0*First[IdentityMatrix[Length[C1]]]};
q0 = P1 /. x -> 0;
P  = Function[z, Join[-Sign[q0]Floor[z.C1/Abs[q0]],Drop[z, -1]]];
P1 = Function[z, Join[-Sign[q0]Floor[z.C1 + Abs[q0] - 1)/Abs[q0]], Drop[z,-1]]];
While[True, L = Union[L, Map[P, L], Map[P1, L]];
If[Length[L] == L1, Print[L1];
Print[‘‘Contractive’’];
Break[]];
L1 = Length[L]; Print[L1]; ];
While[True, L = Union[Map[P, L]];
If[Length[L] == L1, If[Length[L] =!= 1, Print[L1];
Print[‘‘Periodic Elements’’];
Print[‘‘CBP’’];
Break[]; ];];
L1 = Length[L];
Print[L1]; ];
```

References

[1] S. Akiyama, T. Borbèly, H. Brunotte, A. Pethö & J. M. Thuswaldner. Generalized radix representation and dynamical systems I. Acta Math. Hungar. **108**(2005), 207-238.

[2] S. Akiyama, T. Borbèly, H. Brunotte, A. Pethö & J. M. Thuswaldner. On a generalization of the radix representation - a survey. Fields Institute Communication, **41**(2004), 19-27.

[3] S. Akiyama & A. Pethö. On Canonical number systems. Theoret. Comput. Sci. **270**(2002), 921-933.

[4] G. Barat, V. Berthe, P. Liardet & J. M. Thuswaldner. Dynamical Directions in Numeration. Ann. Ist. Fourier Universite Joseph Fourier Grenoble, **56**(2006), 1987-2092.

[5] H. Brunotte. On trinomial bases of radix representation of algebraic integers. Acta Sci. Math. (Szeged) **67**(2001), 521-527.

[6] W. J. Gilbert. Radix representations of quadratic fields. J. Math. Anal. Appl. **83**(1981), 264-274.

[7] V. Grunwald. *Giornale di Matematiche di Battaglini.* (1885), 203-221.

[8] D. M. Kane. Generalized base representations. J. Number Theory 120 (2006), 92-100.

[9] D. E. Knuth. *Art of Computer Programming, Volume 2: Seminumerical Algorithms.* 3rd ed. Addison-Wesley, London 1998.

[10] A. Pethö. Notes on CNS polynomials and integral interpolation. *More Sets, Graphs and Numbers.* Springer-Verlag, Hungary (2006), 301-315.

[11] A. Pethö. On a polynomial transformation and its application to the construction of a public key cryptosystem. In: A. Pethö, M. Pohst, H. G. Zimmer, H. C. Williams, editor. *Computational Number Theory.* Walter de Gruyter, Berlin (1991), 31-43.

[12] K. Scheicher & J. M. Thuswaldner. On the characterization of canonical number systems. Osaka J. Math. **41**(2004). 327-351.