Polynomials with Two Values

Joachim von zur Gathen

AT&T Bell Laboratories
Department of Computer Science, University of Toronto
Toronto, Ontario, Canada M5S 1A4

James R. Roche

AT& T Bell Laboratories
Murray Hill, New Jersey 07974

September 23, 1993

1. Introduction

We consider polynomials $f \in \mathbf{R}[x]$ that take only two values on the domain $\{0, \ldots, n\}$. For each n, we ask how small the degree of such a (nonconstant) polynomial can be. We may assume without loss of generality that the range of f is $\{0, 1\}$. Since arbitrary prescribed values can be interpolated by a polynomial of degree at most n, we may assume that $\deg(f) \leq n$. Then f is uniquely determined, and $f \in \mathbf{Q}[x]$. We seek bounds on the *gap* between $\deg(f)$ and n.

More precisely, for any $n \geq 1$ and $a = (a_0, \ldots, a_n) = (f(0), \ldots, f(n)) \in \mathbf{Q}^{n+1}$, with $f \in \mathbf{Q}[x]$ of degree at most n, we define the *gap* of a as

$$\gamma(a) = n - \deg(f),$$

where the degree of any constant polynomial is taken to be zero. For $n \geq 1$, the *maximal gap* is

$$\Gamma(n) = \max_{a \in A_n} \gamma(a),$$

where

$$A_n = \{0, 1\}^{n+1} \backslash \{(0, \ldots, 0),\ (1, \ldots, 1)\}.$$

As an example, if $a = (1, 0, \ldots, 0)$, then f has at least n zeros (at $1, 2, \ldots, n$) and thus has degree at least n. But $\deg(f) \leq n$, so that $\deg(f) = n$ and $\gamma(a) = 0$.

In Section 2 we characterize the property "$\gamma(a) \geq r$" by r linear equations in $a_0, \ldots, a_n$. Then we note that only an exponentially small fraction of vectors has positive gap, and we exhibit a family of vectors with gap one. In Section 3 we introduce the notion of a *folded vector*. The characterization of the gap then leads to several infinite families of vectors, again with gap one, via the solution of certain Diophantine equations. In Section 4 we extend and combine these examples to obtain families with gap two or three, and then give further examples with gap one in Section 5; the latter do not, however, improve our knowledge of Γ. In Section 6 we report on a computer search which determined all vectors with positive gap for $n \leq 128$; the largest gap is 3. Another computer search found all vectors with gap of 3 or more for $n \leq \{500\}$. Over this range of n, the largest gap is still 3.

The bound $\Gamma(n) < n/2$ is trivial. In Section 7 we show that $\Gamma(n) = 0$ if $n + 1$ is prime; using a bound on the gap between consecutive primes, we then obtain $\Gamma(n) = O(n^{.548})$ in general. A heuristic argument leads us to conjecture that $\Gamma(n) = O(1)$.

This research was motivated by work of Nisan and Szegedy (1992). They investigate the degree of polynomials in $\mathbf{R}[x_1, \ldots, x_n]$ that interpolate (or approximate) a given Boolean function $g : \{0,1\}^n \to \{0,1\}$. The smallest degree of such interpolating polynomials is the *Fourier degree* of g. If g is symmetric, there is an associated function $f: \{0, \ldots, n\} \to \{0,1\}$ whose interpolation problem is equivalent to the original one. Bounds on $\Gamma(n)$ are thus equivalent to bounds on the Fourier degree of symmetric Boolean functions.

2. Simple Bounds on the Gap

We begin by characterizing the gap $\gamma(a)$ in terms of binomial coefficients.

Theorem 2.1: *Let $0 \leq r \leq n$, $a = (a_0, \ldots, a_n) \in \mathbf{Q}^{n+1}$, and let $f \in \mathbf{Q}[x]$ be the unique interpolating polynomial with $\deg(f) \leq n$ and $f(j) = a_j$ for $0 \leq j \leq n$. Then for $0 \leq r \leq n$, the following are equivalent:*

(i) $\gamma(a) \geq r$,

(ii) $\deg(f) \leq n - r$,

(iii) For $n-r<m\le n$, we have

$$\sum_{0\le j\le m} (-1)^j \binom{m}{j} a_j = 0. \tag{2.1}$$

Proof: Recall that $\gamma(a) = n - \deg(f)$, and use induction on r. The case $r=0$ is trivial. So let $r=1$, and for $0\le j\le n$ let

$$g_j = \prod_{\substack{0\le i\le n\\ i\ne j}} (x-i) / \prod_{\substack{0\le i\le n\\ i\ne j}} (j-i) \in \mathbf{Q}[x]$$

be the basic Lagrange interpolating polynomial, with $g_j(i) = \delta_{ij}$ for $0\le i\le n$. Then $f = \sum_{0\le j\le n} a_j g_j$, and $\gamma(a)\ge 1$ if and only if $\deg(f)\le n-1$, which holds if and only if the coefficient of x^n in f is zero. This coefficient is

$$\sum_{0\le j\le n} \Big(\prod_{\substack{0\le i\le n\\ i\ne j}} (j-i)\Big)^{-1} a_j = \sum_{0\le j\le n} \frac{a_j}{j!(-1)^{n-j}(n-j)!} = \frac{(-1)^n}{n!} \sum_{0\le j\le n} (-1)^j \binom{n}{j} a_j.$$

This proves the case $r=1$.

For the induction step, we assume that the theorem holds for $r=t-1$, where $t\ge 2$, and show that the theorem follows for $r=t$. By definition, f is the minimal interpolating polynomial for $a_0,\ldots,a_n$. We note that

$$\deg(f)\le n-t+1 \iff f \text{ is also the (unique) minimal interpolant for } a_0,\ldots,a_{n-t+1}.$$

Now using the case $r=1$ for interpolating at $0,\ldots,n-t+1$ and the induction hypothesis for interpolating at $0,\ldots,n$, we find that

$$\begin{aligned} \deg(f)\le n-t \quad &\iff \quad \deg(f)\le n-t+1 \text{ and} \\ &\qquad\quad (2.1) \text{ holds for } m = n-t+1 \\ &\iff \quad (2.1) \text{ holds for } n-t<m\le n. \qquad \square \end{aligned}$$

Definition 2.2: We have four natural operations on A_n, namely, for $a=(a_0,\ldots,a_n)\in A_n$:

the *reverse* of a: $\overline{a} = (a_n,\ldots,a_0)\in A_n$,

the *complement* of a: $e_n - a = (1-a_0,\ldots,1-a_n)\in A_n$,

the *prefix* of a: $\pi a = (a_0,\ldots,a_{n-1})\in A_{n-1}\cup\{(0,\ldots,0),(1,\ldots,1)\}$,

the *suffix* of a: $\sigma a = (a_1,\ldots,a_n)\in A_{n-1}\cup\{(0,\ldots,0),(1,\ldots,1)\}$, where $e_n = (1, \ldots, 1) \in \mathbf{N}^{n+1}$. If $f \in \mathbf{Q}[x]$ interpolates a, then $f(n-x)$ and $1-f$ interpolate $\overline{a}$ and $e_n - a$, respectively. In particular, $\gamma(a) = \gamma(\overline{a}) = \gamma(e_n - a)$.

We claim that (2.1) entails the following relations:

$$\forall m, i \quad n - r < m \leq n,\ 0 \leq i \leq n - m \qquad \sum_{0 \leq j \leq m} (-1)^j \binom{m}{j} a_{j+i} = 0. \tag{2.2}$$

Using Pascal's triangle

$$\binom{m+1}{j} = \binom{m}{j-1} + \binom{m}{j}, \tag{2.3}$$

this is easily proved by induction on i:

$$\begin{aligned} 0 &= \sum_{0 \leq j \leq m+1} (-1)^j \binom{m+1}{j} a_{j+i} = \sum_{0 \leq j \leq m+1} (-1)^j \left(\binom{m}{j-1} + \binom{m}{j} \right) a_{j+i} \\ &= -\sum_{0 \leq l \leq m+1} (-1)^j \binom{m}{l} a_{l+i+1}. \end{aligned}$$

(2.2), together with Theorem 2.1, implies the following propagation of the gap to and from prefix and suffix vectors, which will be useful in Section 4.

Theorem 2.3: *Let $n \geq 2, r \geq 2$ and $a \in \mathbf{Q}^{n+1}$.*

(i) $\gamma(a) \geq r \iff \gamma((a_0, \ldots, a_{n-i})) \geq r - i$ *for* $0 \leq i \leq r$.

(ii) $\gamma(a) \geq r \iff \gamma(a) \geq 1$ *and* $\gamma(\pi a) \geq r - 1$.

(iii) $\gamma(a) \geq r \iff \gamma(a) \geq 1$ *and* $\gamma(\sigma a) \geq r - 1$.

(iv) $\gamma(a) \geq r \iff \gamma(\pi a) \geq r - 1$ *and* $\gamma(\sigma a) \geq r - 1$.

(v) $\Gamma(n-1) \geq \Gamma(n) - 1$.

Proof: We denote by $\Sigma(m, a)$ the sum in (2.1). For $0 \leq i \leq r$ and $n - r < m \leq n - i$, we have $\Sigma(m, a) = \Sigma(m, (a_0, \ldots, a_{n-i}))$. This implies (i) and (ii). Next, (iii) follows from (ii) applied to $\overline{a}$, since $\gamma(a) = \gamma(\overline{a})$ and $\gamma(\sigma a) = \gamma(\overline{\sigma a}) = \gamma(\pi \overline{a})$. In (iv), "$\Longrightarrow$" follows from (ii) and (iii). For "$\Longleftarrow$", we use

$$\begin{aligned} \Sigma(n, a) &= \sum_{0 \leq j \leq n} (-1)^j \binom{n}{j} a_j = \sum_{0 \leq j \leq n} (-1)^j \binom{n-1}{j-1} a_j + \sum_{0 \leq j \leq n} (-1)^j \binom{n-1}{j} a_j \\ &= \Sigma(n-1, \sigma a) + \Sigma(n-1, \pi a), \end{aligned}$$

so that (iv) follows from (ii). For (v), let $a \in A_n$ with $\Gamma(n) = \gamma(a) = r$. Then $\pi a \in A_{n-1}$ or $\sigma a \in A_{n-1}$, and in either case $\Gamma(n-1) \geq r-1$, by (ii) or (iii). $\square$

The propagation in (v) is illustrated in Table 3 for $n = 15, 35, 63, 99, 105$.

The following corollary provides an alternative characterization of $\gamma(a)$, used in a computer program described in Section 7.

Corollary 2.4: *Let $0 \leq r \leq n$ and $a = (a_0, \ldots, a_n) \in \mathbf{Q}^{n+1}$. Then $\gamma(a) \geq r$ if and only if*

$$\sum_{0 \leq j \leq n+1-r} (-1)^j \binom{n+1-r}{j} a_{j+i} = 0$$

for $0 \leq i \leq r-1$.

We note that in the characterization of Corollary 2.4, we slide a window of fixed width $n+2-r$ across the $n+1$ coefficients $a_0, \ldots, a_n$, while in Theorem 2.1, the window width varies.

We now show that most choices of a have gap equal to zero.

Theorem 2.5: *For each $n \geq 2$ and randomly chosen $a \in A_n$,*

$$\Pr\{\gamma(a) \geq 1\} < 2^{-n/3}.$$

Proof: Let $s = \lfloor n/3 \rfloor + 1$. With arbitrary values a_j for $s \leq j \leq n$, we show that there is at most one choice of the remaining a_j's that satisfies the condition in Theorem 2.1 for $r = 1$. This will follow because the sequence of binomial coefficients is superincreasing in the appropriate sense. Since $s \geq (n+1)/3$, the desired probability is at most

$$\frac{2^{n+1-s}}{\# A_n} \leq \frac{2^{(2n+2)/3}}{2^{n+1}-2} = 2^{-n/3} \frac{2^{2/3}}{2-2^{-n+1}} < 2^{-n/3}$$

for $n \geq 3$. For $n = 2$, the probability is 0, by Table 3.

So now suppose that there are two distinct vectors a and b such that $a_j = b_j$ for $n/3 < j \leq n$ and

$$\sum_{0 \leq j \leq n} (-1)^j \binom{n}{j} a_j = \sum_{0 \leq j \leq n} (-1)^j \binom{n}{j} b_j = 0.$$

Let m be the maximum value of j for which $a_j \neq b_j$, so that $m \leq n/3$. Then

$$\sum_{0 \leq j \leq m} (-1)^j \binom{n}{j} (a_j - b_j) = 0.$$

For each j, let $u_j = (-1)^j (a_j - b_j)/(a_m - b_m)$. Then

$$u_j \in \{-1, 0, 1\}, \quad u_m = (-1)^m, \quad \text{and} \quad \sum_{0 \leq j \leq m} \binom{n}{j} u_j = 0.$$

Thus

$$\binom{n}{m} = (-1)^{m+1} \sum_{0 \leq j < m} \binom{n}{j} u_j \leq \sum_{0 \leq j < m} \binom{n}{j}. \tag{2.4}$$

But for $0 \leq j < m$, we have

$$\binom{n}{j} \binom{n}{j+1}^{-1} = \frac{j+1}{n-j} \leq \frac{m}{n-m+1} \leq \frac{n/3}{\frac{2n}{3}+1} < \frac{1}{2}.$$

Therefore

$$\sum_{0 \leq j < m} \binom{n}{j} < \binom{n}{m} \sum_{0 \leq j < m} (1/2)^{m-j} < \binom{n}{m} \cdot 1,$$

contradicting (2.4). $\square$

For $n \geq 2$, we have the following trivial bounds on the maximal gap:

$$0 \leq \Gamma(n) \leq \frac{n-1}{2},$$

since for each $a \in A_n$, with interpolating polynomial $f \in \mathbf{Q}[x]$, either f or $f-1$ has at least $(n+1)/2$ zeros in $\{0, 1, \ldots, n\}$; since f is not constant, we have $\deg(f) = \deg(f-1) \geq (n+1)/2$. We also have the following simple example of a positive gap.

Theorem 2.6: *Let $n \geq 3$ be odd and $a \in A_n$ with $a_j = a_{n-j}$ for $0 \leq j \leq n$. Then*

$$\gamma(a) \geq 1.$$

Proof: This follows from Theorem 2.1, with $r = 1$. $\square$

Observation 2.7: Since the sum in (2.1) is linear in the a_j's, it is clear that any two (or more) solution vectors can be added componentwise to yield another vector with positive gap. The only restriction is that the new vector must also have its components in $\{0, 1\}$. Thus the set of $2^{(n+1)/2} - 2$ nontrivial vectors a in Theorem 2.6 can be described as the set of all admissible sums of the $(n+1)/2$ "basis" vectors $(1, 0, 0, \ldots, 0, 0, 1)$, $(0, 1, 0, 0, \ldots, 0, 0, 1, 0)$, $\ldots$, $(0, \ldots, 0, 1, 1, 0, \ldots, 0)$.

3. Folded Vectors and Examples with Gap One

In this section and the next two we exhibit several infinite families of vectors with positive gap. Three of the families have gap two, and two families have gap three.

Because of the symmetry

$$\binom{n}{j} = \binom{n}{n-j}, \tag{3.1}$$

it is convenient to "fold" each vector $a \in A_n$ back on itself and consider the shortened vector $\varphi(a)$ defined below.

Definition 3.1: For $n \geq 2$ and $a \in A_n$, we define the *folded vector* $\varphi(a)$ as follows:

$$b = (b_0, \ldots, b_s) = \varphi(a) = \begin{cases} (a_0 - a_n,\ a_1 - a_{n-1},\ \ldots, a_{(n-1)/2} - a_{(n+1)/2}) & \text{if } n \text{ is odd,} \\ (a_0 + a_n,\ a_1 + a_{n-1},\ \ldots, a_{(n-2)/2} + a_{(n+2)/2}) & \text{if } n \text{ is even,} \end{cases}$$

where $s = \lfloor (n-1)/2 \rfloor$. We denote this mapping by the *folding operator* $\varphi : A_n \to B_n \subset \mathbf{Z}^{s+1}$, where

$$B_n = \varphi(A_n) = \begin{cases} \{-1, 0, 1\}^{(n+1)/2} & \text{if } n \text{ is odd,} \\ \{0, 1, 2\}^{n/2} & \text{if } n \text{ is even.} \end{cases}$$

Observation 3.2: If n is even, we have an additional component $a_{n/2}$ in a, which does not appear in $\varphi(a)$. However, we may usually assume without loss of generality that $a_{n/2} = 0$. Otherwise, the complementary vector $e_n - a$ has $(e_n - a)_{n/2} = 0$ and $\varphi(e_n - a) = 2e_{(n-2)/2} - \varphi(a)$.

In this notation, Theorem 2.1 with $r = 1$ says that $\gamma(a) \geq 1$ for an $a \in A_n$ (with $a_{n/2} = 0$ if n is even) if and only if

$$\sum_{0 \leq j \leq s} (-1)^j \binom{n}{j} b_j = 0, \tag{3.2}$$

where $b = \varphi(a)$ and $s = \lfloor (n-1)/2 \rfloor$. This is the property that we will work with in the sequel, and if $b \in B_n$ satisfies (3.2), we say that b *has positive gap*. In particular, if $b \in B_n$ has positive gap, then $\gamma(a) \geq 1$ for every $a \in \varphi^{-1}(\{b\})$. On the other hand, for any $a \in A_n$ with $\gamma(a) > 0$, either $b = \varphi(a)$ or, if n is even and $a_{n/2} = 1$, $b = \varphi(e_n - a)$ has positive gap.

Observation 3.3: If n is odd, $a \in A_n$, and $b = \varphi(a) \in B_n$, then $-b = \varphi(\overline{a}) = \varphi(e_n - a) \in B_n$. Thus b has positive gap if and only if $-b$ does.

Observation 3.4: For $i \in \{0,1\}$ and $b \in B_n$, we let $w_i(b)$ be the number of components in b that equal i. If n is odd, then $\#\varphi^{-1}(\{b\}) = 2^{w_0(b)}$, and if n is even, then $\#\varphi^{-1}(\{b\}) = 2^{w_1(b)+1}$, because $a_{n/2}$ can be 0 or 1. (3.2) will guide our search for nontrivial gaps. However, the actual gap $\gamma(a)$ cannot be determined from $\varphi(a)$ alone. This is illustrated by the vectors $a^{(1)}$, $a^{(2)}$, $a^{(3)}$, defined after Theorem 4.1, and πa from Theorem 4.1, which have the same folded vector but gaps $2,1,1,2$, respectively. Given $b \in B_n$, it is easy to construct $\varphi^{-1}(\{b\})$. This may, however, be a large set, and working with the single folded vector b is advantageous, both conceptually (see the theorems below) and computationally (see Section 6). Note in particular that

$$\#B_n \approx 3^{n/2} \ll 2^n \approx \#A_n.$$

We now use our "folded vector" notation to describe several more infinite families of vectors with gap one. Our basic idea is to take $b \in B_n$ with $b_j = 0$ for all but a small number of consecutive values of j. Then (3.2) is equivalent to a Diophantine equation in n and k of small degree whose solutions we can determine. Our examples in Section 4 of gap two and three are based on these families.

In the simplest nontrivial case, we have $b_j = 0$ for all values of j but k and $k+1$, where $0 \le k \le s-1 = \lfloor (n-1)/2 \rfloor - 1$. Then we can rewrite (3.2) as follows:

$$\begin{aligned} 0 &= \sum_{0 \le j \le s} (-1)^j \binom{n}{j} b_j = (-1)^k \binom{n}{k} b_k + (-1)^{k+1} \binom{n}{k+1} b_{k+1} \\ &= (-1)^{k+1} \frac{n!}{(k+1)!(n-k)!} \Big((n-k) b_{k+1} - (k+1) b_k \Big). \end{aligned}$$

If n is odd, then b_k, $b_{k+1} \in \{-1, 1\}$, and the only possible solution has $b_k = b_{k+1}$ and $n = 2k+1$. But this violates the requirement that $k \le s-1$.

If n is even, then b_k, $b_{k+1} \in \{1, 2\}$. But $k+1 \le s$, so that $\binom{n}{k} < \binom{n}{k+1}$ and the only possible solution is $b_k = 2$, $b_{k+1} = 1$. We find all solutions to this equation in the next theorem.

Theorem 3.5: *Let n be even, $0 \le k \le (n-4)/2$, and $b \in B_n$ with $b_k = 2$, $b_{k+1} = 1$, and $b_j = 0$ otherwise. Then b has positive gap if and only if*

$$n = 6t + 2 \ \text{ and } \ k = 2t \ \text{ for some } \ t \ge 1.$$

Proof: By the above, it is sufficient to find all solutions to the equation

$$2(k+1) = n - k.$$

Then $n = 3k+2$. Since n is even, we have $k = 2t$ and $n = 6t+2$ for some $t \geq 0$. This solution satisfies $k \leq (n-4)/2$ if and only if $t \geq 1$. $\square$

Corollary 3.6: *For each $b \in B_n$ as in Theorem 3.5, we have $\#\varphi^{-1}(\{b\}) = 4$, and for each of the two $a \in \varphi^{-1}(\{b\})$ with $a_{n/2} = 0$, we have $\gamma(a) = 1$.*

Proof: Observation 3.4 implies the first claim. It is straightforward to check that neither of the two vectors $a \in \varphi^{-1}(\{b\})$ with $a_{n/2} = 0$ satisfies (2.1) with $r = 2$; thus $\gamma(a) < 2$. $\square$

If we allow $b \in B_n$ to have *three* consecutive nonzero components, we obtain a second-order Diophantine equation in n and k. So suppose that all components of b except b_{k-1}, b_k, b_{k+1} are zero. Then (3.2) is equivalent to

$$(-1)^{k-1}\binom{n}{k-1}b_{k-1} + (-1)^k\binom{n}{k}b_k + (-1)^{k+1}\binom{n}{k+1}b_{k+1} = 0,$$

or, equivalently,

$$(n-k+1)(n-k)b_{k-1} - (n-k+1)(k+1)b_k + (k+1)k\ b_{k+1} = 0.$$

Writing $m = n - k$, (3.2) is equivalent to

$$(m+1)m\ b_{k-1} - (m+1)(k+1)\ b_k + (k+1)k\ b_{k+1} = 0. \tag{3.3}$$

Because $k < m$, we can quickly rule out most values of (b_{k-1}, b_k, b_{k+1}) as solutions. We find that if n is even, then (b_{k-1}, b_k, b_{k+1}) equals $(1,2,1)$, and that if n is odd, then it equals $(-1,1,1)$ or $(1,-1,-1)$. The two possibilities for odd n correspond to pairs of unfolded vectors in A_n that are reverses of each other, as discussed in Observation 3.3. The complete solutions are given in the next two theorems.

Theorem 3.7: *Let n be even, $1 \leq k \leq (n-4)/2$, and $b \in B_n$ with $b_{k-1} = b_{k+1} = 1$, $b_k = 2$, and $b_j = 0$ otherwise. Then b has positive gap if and only if*

$$n = 4t^2 - 2 \quad \textit{and} \quad k = 2t^2 - t - 1 \quad \textit{for some} \quad t \geq 2.$$

Proof: Letting $m = n - k$ and using (3.3), we have to find all integral solutions with $1 \le k < m$ of the equation

$$(m+1)m - 2(m+1)(k+1) + (k+1)k = 0.$$

Solving for m, we obtain

$$m = \frac{(2k+1) \pm \sqrt{8k+9}}{2}.$$

Thus $8k + 9 = u^2$ for some $u \in \mathbf{N}$, from which it follows that

$$m = \frac{u^2 \pm 4u - 5}{8}.$$

Since $m \in \mathbf{N}$, it follows that u is odd, say $u = 2v - 1$ for some $v \in \mathbf{N}$. Then

$$k = \frac{v^2 - v - 2}{2} \quad \text{and} \quad m = \frac{(v^2 - v - 1) \pm (2v - 1)}{2}.$$

Since $m > k$, we have

$$m = \frac{(v^2 - v - 1) + (2v - 1)}{2} = \frac{v^2 + v - 2}{2}.$$

Then $n = k + m = v^2 - 2$. Since n is even, we have $v = 2t$ for some $t \in \mathbf{N}$. Thus we obtain

$$n = 4t^2 - 2, \quad k = 2t^2 - t - 1, \quad m = n - k = 2t^2 + t - 1.$$

One checks that this solution is valid for all $t \ge 2$, but not for $t = 1$. $\square$

The Fibonacci numbers are given by $F_0 = 0$, $F_1 = 1$, and $F_i = F_{i-1} + F_{i-2}$ for $i \ge 2$.

Theorem 3.8: *Let n be odd, $1 \le k \le (n-3)/2$, and $b \in B_n$ with $b_{k-1} = -1$, $b_k = b_{k+1} = 1$, and $b_j = 0$ otherwise. Then b has positive gap if and only if*

$$n = F_{2i+2}F_{2i+3} - 1 \text{ and } k = F_{2i}F_{2i+3} \text{ for some } i \ge 2 \text{ with } i \not\equiv 1 \bmod 3.$$

Proof: We seek all solutions to the equation

$$\binom{n}{k+1} = \binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}.$$

This problem has been solved by several authors using standard techniques for Pell equations; see, e.g., Singmaster (1975) and Tovey (1985). In Singmaster (1975) it is shown that (n, k) is a solution if and only if

$$n = F_{2i+2}F_{2i+3} - 1 \quad \text{and} \quad k = F_{2i}F_{2i+3} \quad \text{for some } i \geq 0.$$

In addition, we require that n be odd and that $k \geq 1$, so $i \geq 1$ and either F_{2i+2} or F_{2i+3} is even. Since F_j is even if and only if $j \equiv 0 \bmod 3$, it follows that the general solution is valid for our purposes if and only if $i \geq 1$ and $i \not\equiv 1 \bmod 3$. $\square$

Theorem 3.8 shows that $\Gamma(n) \geq 1$ for $n = 103, 731, \ldots$. However, we already know from Theorem 2.6 that $\Gamma(n) \geq 1$ for all odd $n \geq 3$.

So far we have considered the first- and second-order Diophantine equations that arise if all but two or three consecutive components of the folded vector b are zero. We could continue in this vein by letting four consecutive components be nonzero, but third-order Diophantine equations do not usually yield infinite families of solutions. One exception is given by the following theorem.

Theorem 3.9: *Let n be odd, $2 \leq k \leq (n-3)/2$, and $b \in B_n$ with $b_{k-2} = b_{k-1} = 1$, $b_k = b_{k+1} = -1$, and $b_j = 0$ otherwise. Then b has positive gap if and only if*

$$n = 4t^2 - 3 \quad \textit{and} \quad k = 2t^2 - t - 1 \quad \textit{for some} \quad t \geq 2.$$

Proof: We have

$$\begin{aligned}
(-1)^k \sum_{0 \leq j \leq (n-1)/2} (-1)^j \binom{n}{j} b_j &= \binom{n}{k-2} - \binom{n}{k-1} - \binom{n}{k} + \binom{n}{k+1} \\
&= \binom{n}{k-2} + \binom{n}{k-1} - 2\left(\binom{n}{k-1} + \binom{n}{k}\right) + \binom{n}{k} + \binom{n}{k+1} \\
&= \binom{n+1}{k-1} - 2\binom{n+1}{k} + \binom{n+1}{k+1}.
\end{aligned}$$

By Theorem 3.7, this expression is zero only if

$$n + 1 = 4t^2 - 2 \quad \text{and} \quad k = 2t^2 - t - 1 \quad \text{for some} \quad t \geq 1.$$

Moreover, this solution is valid for all $t \geq 2$. $\square$

4. Families with Gap Two or Three

In this section we use Theorem 2.1 with $r \geq 2$ to find families with gap two or three. Theorem 2.3 (v) says that for gap two we need positive gaps for two consecutive values of n. This occurs, e.g., in Theorems 3.7 and 3.9. The next theorem gives the gaps of the corresponding vectors. We use the notation introduced in Definition 2.2 to represent prefix and suffix vectors.

Theorem 4.1: *Let $t \geq 2$, $n = 4t^2 - 1$, $k = 2t^2 - t - 1$, and $a \in A_n$ with $a_k = a_{k+1} = a_{n-k-1} = a_{n-k} = 1$, and $a_j = 0$ otherwise. Then*

(i) $\gamma(a) = 3$,

(ii) $\gamma(\pi a) = 2$,

(iii) $\gamma(\pi\pi a) = 1$.

Proof: Let $a' = \pi\pi a = (a_0, \ldots, a_{n-2}) \in A_{n-2}$. Then $b = -\varphi(a') \in B_{n-2}$ satisfies Theorem 3.9, and thus $\gamma(a') \geq 1$. Theorem 2.3 (ii) and Theorem 3.7 imply the lower bound on $\gamma(\pi a)$ in (ii). By Theorem 2.6, we have $\gamma(a) \geq 1$, and hence $\gamma(a) \geq 3$, using the lower bound in (ii) and Theorem 2.3 (ii). Finally, the sum (2.1) for $m = n - 3$ is

$$(-1)^k \cdot \left(-\binom{n-3}{k-3} + \binom{n-3}{k-2} + \binom{n-3}{k} - \binom{n-3}{k+1} \right).$$

Substituting for n and k, one finds that the sum is nonzero for all t; this implies all the upper bounds, by Theorem 2.3 (ii). $\square$

This approach suggests considering some other vectors, with $n = 4t^2 - 2$ and $k = 2t^2 - t - 1$:

$$\begin{array}{llllllllll}
a^{(1)} = (\ldots & 1 & 1 & 0 & \ldots & 1 & 1 & 0 & \ldots) & \in A_n, \\
a^{(2)} = (\ldots & 0 & 1 & 0 & \ldots & 1 & 1 & 1 & \ldots) & \in A_n, \\
a^{(3)} = (\ldots & 1 & 1 & 1 & \ldots & 0 & 1 & 0 & \ldots) & \in A_n, \\
a^{(4)} = (\ldots & 1 & 1 & 0 & \ldots & 1 & 1 & 0 & \ldots 0\,) & \in A_{n+1}, \\
a^{(5)} = (\ldots & 0 & 1 & 1 & \ldots & 0 & 1 & 1 & \ldots 0\,0\,) & \in A_{n+2}, \\
 & {\scriptstyle k-1} & {\scriptstyle k} & {\scriptstyle k+1} & & {\scriptstyle n-k-1} & {\scriptstyle n-k} & {\scriptstyle n-k+1} & &
\end{array}$$

Now $a^{(1)} = \pi a^{(4)}$, $a^{(2)} = \overline{a^{(3)}}$, and $a = \pi a^{(5)}$ is as in Theorem 4.1. Then one checks, using the method of Theorem 4.1 and additional calculations for the last four upper bounds, that

$$\gamma(a^{(1)}) = 2,\ \gamma(a^{(2)}) = \gamma(a^{(3)}) = 1,\ \gamma(a^{(4)}) = \gamma(a^{(5)}) = 0.$$

Emboldened by our success in finding vectors with gaps of two or three arising from the basic solution of Theorem 3.7, we now try to extend Theorems 3.5 and 3.8 in the same way.

We already noted in Corollary 3.6 that for every $t \geq 1$ and $n = 6t+2$, each of the unfolded vectors corresponding to the (folded) solution vectors of that theorem has gap one. A similar argument shows that we cannot obtain a vector with gap two or more (or even with gap one) and $n = 6t+3$ by appending a trailing zero to either of the two unfolded vectors with gap one in Corollary 3.6.

Turning to Theorem 3.8, we see that for each admissible value of n, the folded vector b satisfying (3.1) has 3 ones and $(n-5)/2$ zeros. Since n is odd, each such b gives rise to $2^{w_0(b)} = 2^{(n-5)/2}$ different unfolded vectors $a \in A_n$. It is well-nigh hopeless to check with our methods for each of these vectors whether $\gamma(a) \geq 2$. It is not difficult, though, to determine whether two of these solutions (or one of these solutions and one of the symmetric solutions for odd n in Theorem 2.6) can be spliced together using Corollary 2.4 to yield a slightly longer vector having gap of two or more.

We seek a vector $a = (a_0, \ldots, a_{n+1}) \in A_{n+1}$ such that both folded vectors $\varphi(\pi a)$ and $\varphi(\sigma a) \in B_n$ are derived from Theorem 2.6 or Theorem 3.8.

If πa and σa both satisfy the symmetry condition of Theorem 2.6, then $a_{n-j} = a_j = a_{n+2-j}$ for $1 \leq j \leq n$. Using the fact that n is odd, we find that $a_0 = a_1 = \cdots = a_{n+1}$, contradicting the assumption that $a \in A_{n+1}$. A similar argument shows that πa and σa cannot both correspond to solutions of Theorem 3.8.

A somewhat more complicated argument shows that for each n as in Theorem 3.8, there is essentially just one way to choose $\sigma a, \pi a$ satisfying Theorem 2.6 and/or Theorem 3.8 to create $a \in A_{n+1}$ with $\gamma(a) \geq 2$. This solution is given in the following theorem.

The proof below will use the fact that alternating sums of binomial coefficients can be collapsed as follows, for any $0 \le k \le \ell \le n$ with $n \ge 1$:

$$\begin{aligned} \sum_{k\le j\le \ell} (-1)^j \binom{n}{j} &= \sum_{k\le j\le \ell} (-1)^j \left(\binom{n-1}{j-1} + \binom{n-1}{j} \right) \\ &= (-1)^k \binom{n-1}{k-1} + (-1)^\ell \binom{n-1}{\ell}. \end{aligned} \tag{4.1}$$

As usual, $\binom{n-1}{-1}$ and $\binom{n-1}{n}$ have to be interpreted as zero, and $\binom{0}{0}$ as one.

Theorem 4.2: *Let $i \ge 2$ with $i \not\equiv 1 \bmod 3$, $n = F_{2i+2}F_{2i+3} + 1$, $k = F_{2i}F_{2i+3}$, and let $a \in A_n$ be given by*

$$a = \begin{cases} (0,1,0,1,\ldots,1,0,\underbrace{1}_{k},\underbrace{1}_{k+1},0,0,\ldots,0,0,\underbrace{1}_{n-k-1},\underbrace{1}_{n-k},0,1,,\ldots,1,0) & \text{if } k \text{ is odd,} \\ (1,0,1,0,\ldots,1,0,\underbrace{1}_{k},\underbrace{1}_{k+1},0,0,\ldots,0,0,\underbrace{1}_{n-k-1},\underbrace{1}_{n-k},0,1,\ldots,0,1) & \text{if } k \text{ is even.} \end{cases}$$

$$a = \begin{cases} (\underset{0}{0},\ 1,0,1,\ldots,1,0,\ \underset{k}{1},\ \underset{k+1}{1},\ 0,0,\ldots,0,0,\ \underset{n-k-1}{1},\ \underset{n-k}{1},\ 0,1,\ldots,1,\ \underset{n}{0}) & \text{if } k \text{ is odd,} \\ (1,\ 0,1,0,\ldots,1,0,\ 1,\ 1,\ 0,0,\ldots,0,0,\ 1,\ 1,\ 0,1,\ldots,0,\ 1) & \text{if } k \text{ is even.} \end{cases}$$

Then n is odd, and the following hold.

(i) $\gamma(a) = 3$.

(ii) $\gamma(\pi a) = \gamma(\sigma a) = 2$.

Proof: Both a and $\sigma\pi a = \pi\sigma a$ are symmetric, hence have gap at least one by Theorem 2.6. If k is odd, then $b = \varphi(\sigma\sigma a)$ satisfies Theorem 3.8, so that $\gamma(\sigma\sigma a) \ge 1$ as well, and then $\gamma(\sigma a) \ge 2$ and $\gamma(a) \ge 3$, by Theorem 2.3 (iii) and (iv). If k is even, then $b = \varphi(\pi\pi a)$ satisfies Theorem 3.8, so that $\gamma(\pi a) \ge 2$ and $\gamma(a) \ge 3$, again by Theorem 2.3. This shows all lower bounds.

Finally, it is sufficient to show that $\gamma(\sigma\pi\pi a) = 0$; this implies all claimed upper bounds by Theorem 2.3 (iv). For odd k, Theorem 2.1 implies that $\gamma(\sigma\pi\pi a) > 0$ if and only if the following sum is nonzero:

$$\begin{aligned}\sum_{0\le j\le n-3}(-1)^j\binom{n-3}{j}a_{j+1} &= \sum_{0\le j\le k}(-1)^j\binom{n-3}{j}+\binom{n-3}{k-1}\\ &= \binom{n-4}{k-2}+\binom{n-4}{k-1}-\binom{n-4}{k},\end{aligned}$$

using (3.1) and (4.1). The last sum is nonzero by Theorem 3.8.

A similar calculation establishes the theorem for even k. $\square$

We summarize our main results so far, namely the lower bounds on $\Gamma(n)$, in Table 1, where $t \geq 2$ and $i \geq 2$ satisfies $i \not\equiv 1 \bmod 3$.

bound on $\Gamma(n)$	n	first five values	reference
≥ 1	$2t-1$	3,5,7,9,11	Theorem 2.6
≥ 1	$6t-4$	8, 14, 20, 26, 32	Theorem 3.5
≥ 2	$4t^2-2$	14, 34, 62, 98, 142	Theorem 4.1 (ii)
≥ 3	$4t^2-1$	15, 35, 63, 99, 143	Theorem 4.1 (i)
≥ 2	$F_{2i+2}F_{2i+3}$	104, 714, 33552, 229970, 10803704	Theorem 4.2 (ii)
≥ 3	$F_{2i+2}F_{2i+3}+1$	105, 715, 33553, 229971, 10803705	Theorem 4.2 (i)

Table 1: Lower bounds on Γ.

5. More vectors with gap one

In this section we present new families with nontrivial gaps; however, these results do not improve the lower bounds given previously.

Because $\gamma(a) = 2$ for the vectors σa and $\pi a \in A_{n-1}$ given in Theorem 4.2, the folded vectors have positive gap. Thus *every* vector $a' \in A_{n-1}$ with the same folded vector has positive gap. We give a direct proof for a particular example that will lead us to a new family of vectors with positive gap.

Theorem 5.1: *Let $i \geq 2$ with $i \not\equiv 1 \bmod 3$, $n = F_{2i+2}F_{2i+3}$, $k = F_{2i}F_{2i+3}$, and $b \in B_n$ with $b_j = 1$ for $j \in \{0, \ldots, k-1\} \cup \{k+1\}$, $b_k = 2$, and $b_j = 0$ otherwise. Then b has positive gap.*

Proof: From Theorem 3.8 we know that n is even, so that indeed $b \in B_n$.

$$\begin{aligned}\sum_{0\le j\le (n-2)/2} (-1)^j \binom{n}{j} b_j &= \sum_{0\le j\le k+1} (-1)^j \binom{n}{j} + (-1)^k \binom{n}{k} \\ &= (-1)^{k+1}\binom{n-1}{k+1} + (-1)^k \binom{n-1}{k-1} + (-1)^k \binom{n-1}{k},\end{aligned}$$

using (4.1). Theorem 3.8 shows that this final expression equals zero. □

Corollary 5.2: *For $n, k \in \mathbf{N}$, the equation*

$$\binom{n}{k} = \sum_{0\le j\le k+1} (-1)^{k+1-j} \binom{n}{j}$$

holds if and only if $n = F_{2i+2}F_{2i+3}$ and $k = F_{2i}F_{2i+3}$ for some $i \ge 1$.

Proof: The proof follows from Singmaster (1975) and the identity derived in Theorem 5.1. There is no parity constraint on n here, hence no constraint on i modulo 3. □

The telescoping trick (4.1) can be used to reduce the sum in (3.1) to a low-degree Diophantine equation whenever the folded vector b begins with a string of ones (or a string of twos), then has a few arbitrary components, and ends with a string of zeros.

A check of the various possibilities reveals that there are just two essentially different families of these vectors that yield Diophantine equations of first or second order having nontrivial solutions. The first family was given in Theorem 5.1; the other family will be given in the following theorems.

Theorem 5.3: *Let $1 \le k \le n-2$. Then the following three properties are equivalent.*

$$\binom{n}{k+1} - \binom{n}{k} = \sum_{0\le j<k} (-1)^{k-1-j} \binom{n}{j}, \tag{5.1}$$

$$\binom{n-1}{k+1} = 2\binom{n-1}{k-1}, \tag{5.2}$$

$$\exists r \ge 1 \quad \begin{pmatrix} u_r \\ v_r \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}^r \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad n = (u_r + v_r)/2, \quad k = (v_r - 1)/2. \tag{5.3}$$

Proof: The equivalence of the first two equations follows from (4.1), and (5.2) is equivalent to

$$\begin{aligned}
&\frac{(n-1)!}{(k+1)!(n-k)!}\Big((n-k)(n-k-1)-2(k+1)k\Big)=0\\
\Longleftrightarrow\quad &(m+1)m=2(k+1)k\\
\Longleftrightarrow\quad &4m^2+4m+2=8k^2+8k+2\\
\Longleftrightarrow\quad &(2m+1)^2+1=2(2k+1)^2,
\end{aligned}$$

where $m=n-k-1$, so that $1 \le m \le n-2$.

Let $u=2m+1$, $v=2k+1$, so that $u \ge 3$ and $v \ge 3$. Then (5.2) is equivalent to

$$u^2-2v^2=-1. \tag{5.4}$$

We will find all integral solutions to (5.4) with $u, v \ge 0$, and then determine which of these solutions yield admissible m and k. First we note that $uv \neq 0$, and that (u,v) satisfies (5.4) if and only if

$$(u', v')=(3u-4v, -2u+3v) \tag{5.5}$$

also satisfies (5.4).

If $u \ge 5$ and $v \ge 1$, then, since $u^2-2v^2=-1$, we have

$$\frac{-u^2}{25} \le u^2-2v^2<0,$$

from which it follows that $4/3<u/v<3/2$. Thus $0<u'<u$ and $0<v'<v$. Therefore any solution to (5.4) with $u \ge 5, v \ge 1$ yields another solution (u', v') with $1 \le u' < u$ and $1 \le v' < v$.

After a finite number of applications of the reduction above, we obtain a *fundamental* solution (u_0, v_0) with $1 \le u_0 \le 4$ and $v_0 \ge 1$. The only solution of this form is $(u_0, v_0) = (1,1)$. Inverting (5.5), we find that $(u,v)=(u_r, v_r)$ for some $r \ge 0$, where

$$\begin{pmatrix} u_r \\ v_r \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}^r \begin{pmatrix} 1 \\ 1 \end{pmatrix}. \tag{5.6}$$

On the other hand, an induction shows that each (u_r, v_r) actually satisfies (5.4), so that (5.6) gives the set of all solutions to (5.4) in nonnegative integers.

Returning to the Diophantine equation in m and k, we note that u_r and v_r are odd for each r and that $u_r, v_r \ge 3$ for all $r \ge 1$. Letting $m=(u_r-1)/2$, $k=(v_r-1)/2$, and $n=k+m+1$, we find that (5.2) is equivalent to (5.3). $\square$

Now we use Theorem 5.3 to identify another infinite family of vectors with positive gap. It is easily shown that $u_r \geq v_r + 12$ for all $r \geq 2$, so it follows from (5.3) that $k < (n-4)/2$ for all solutions in Theorem 5.3 with $r \geq 2$. Thus (5.1) corresponds to a legitimate folded vector, provided that n is odd.

Theorem 5.4: *Let $r \geq 2$ be even,*

$$n = n_r = \frac{4+3\sqrt{2}}{8}\,(3+2\sqrt{2})^r + \frac{4-3\sqrt{2}}{8}\,(3-2\sqrt{2})^r,$$

$$k = k_r = \frac{2+\sqrt{2}}{8}\,(3+2\sqrt{2})^r + \frac{2-\sqrt{2}}{8}\,(3-2\sqrt{2})^r - \frac{1}{2},$$

and $b \in B_n$ with $b_j = 1$ for $0 \leq j < k$, $b_k = b_{k+1} = -1$, and $b_j = 0$ otherwise. Then $n, k \in \mathbf{N}$, n is odd, and b has positive gap.

Proof: b has positive gap if and only if n is odd and (n,k) satisfies (5.1). Examining $u_r \bmod 4$ and $v_r \bmod 4$ in Theorem 5.3, we see that n is odd if and only if r is even. Diagonalizing the matrix in (5.6), with eigenvalues $e_1 = 3+2\sqrt{2}$ and $e_2 = 3-2\sqrt{2}$, we find that

$$\begin{pmatrix} u_r \\ v_r \end{pmatrix} = \begin{pmatrix} \frac{1+\sqrt{2}}{2} & \frac{1-\sqrt{2}}{2} \\ \frac{2+\sqrt{2}}{4} & \frac{2-\sqrt{2}}{4} \end{pmatrix} \cdot \begin{pmatrix} e_1 & 0 \\ 0 & e_2 \end{pmatrix}^r \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

for all $r \geq 0$. Thus b has positive gap for $(n,k) = (n_r, k_r)$. $\square$

Remark: Theorem 5.4 shows that $\Gamma(n) \geq 1$ for $n = 35,\ 1189, \ldots,$ where each value of n in the sequence is about 34 times as great as it predecessor. We already know from Theorem 2.6, however, that $\Gamma(n) \geq 1$ for all odd n.

To conclude this section, we recall Observation 2.7 on linear superposition of solutions. If the folded vectors $b^{(1)}, \ldots, b^{(m)} \in B_n$ satisfy (3.2), then so does every linear combination

$$b = \sum_{1 \leq i \leq m} \lambda_i b^{(i)}, \quad \text{where} \quad \lambda_i \in \mathbf{Z} \ \text{ for all } i.$$

If $b \in B_n$, then it is a folded vector with positive gap. In particular, as we shall see, the solutions of Theorems 3.5 and 3.8 can be combined to yield a new solution when $n = 6t+2 = 4u^2 - 2$ for some $t \geq 1$ and $u \geq 2$.

Theorem 5.5: *Let $u \geq 4$ with $u \not\equiv 0 \bmod 3$, $n = 4u^2 - 2$, $k = (4u^2-4)/3$, $m = 2u^2 - u - 1$, and $b \in B_n$ with $b_k = b_m = 2$, $b_{k+1} = b_{m-1} = b_{m+1} = 1$, and $b_j = 0$ otherwise. Then b has positive gap.*

Proof: We add the solutions of Theorems 3.5 and 3.7 componentwise. Setting $6t + 2 = 4u^2 - 2$, we get the constraint $u \not\equiv 0 \bmod 3$, which insures that $n \equiv 2 \bmod 6$, as required for Theorem 3.5. Then $k = 2t = (n-2)/3 = (4u^2-4)/3$. It is easily verified that $m - 1 > k + 1$ for all $u \geq 3$ (but not for $u = 2$), so that the five nonzero components of b occur in different positions. Thus $b \in B_n$, and the theorem follows by linearity. $\square$

As discussed in Observation 2.7, we can linearly combine vectors $b^{(1)}, \ldots, b^{(m)}$ that satisfy (3.2) for some n even if $b^{(i)} \notin B_n$ for some i, as long as the *linear combination* of the vectors has every component in $\{-1, 0, 1\}$ (for odd n) or in $\{0, 1, 2\}$ (for even n).

As we shall see in the next theorem and in the examples of Section 6, some folded vectors b with positive gap are most naturally expressed as $b^{(1)} + b^{(2)}$, where $b^{(1)} \in B_n$ is a vector with positive gap (a "real solution" of (3.2)), but $b^{(2)} \notin B_n$ is only a "virtual solution" of (3.2).

Lemma 5.6: *Let $t \geq 1$, $n = 6t + 5$, $\ell = 2t + 1$, $s = (n-1)/2$, and $b = (b_0, b_1, \ldots, b_s)$ with $b_\ell = 2$, $b_{\ell+1} = 1$, and $b_j = 0$ otherwise. Then $b \notin B_n$, but b satisfies (3.2); that is, b is a "virtual solution" of (3.2).*

Proof: Since n is odd and $b_\ell = 2 \notin \{-1, 0, 1\}$, we see that $b \notin B_n$. However, the proof of Theorem 3.5 shows that b satisfies (3.2). Furthermore, $\ell + 1 \leq (n-1)/2$ for all $t \geq 0$. $\square$

Combining the "real solutions" of Theorem 5.4 with the "virtual solutions" of Lemma 5.6, we have the following result.

Theorem 5.7: *Let r, $n = n_r$, and $k = k_r$ be as in Theorem 5.4, with $r \equiv 2 \bmod 4$, let $\ell = (n-2)/3$, and $b \in B_n$ defined by*

$$b_j = \begin{cases} 1 & \text{if } j \in \{0, \ldots, k-1\} \backslash \{\ell, \ell+1\}, \\ 0 & \text{if } j \in \{\ell+1\} \cup \{k+2, \ldots, (n-1)/2\}, \\ -1 & \text{if } j \in \{\ell, k, k+1\}. \end{cases}$$

Then $n \equiv 5 \bmod 6$, and b has positive gap.

Proof: Returning to Theorem 5.3 and computing $u_r \bmod 12$ and $v_r \bmod 12$, we find that n has the form $6t + 5$ if and only if $r \equiv 2 \bmod 4$. Now $b = b^{(1)} - b^{(2)}$, where $b^{(1)} = (1, \ldots, 1, -1, -1, 0, \ldots, 0)$ with $b_k^{(1)} = b_{k+1}^{(1)} = -1$ is the solution of Theorem 5.4, and $b^{(2)}$ the virtual solution of Lemma 5.6, with $\ell = (n-2)/3$.

We need only check that the two nonzero components of the virtual solution fall within the string of ones in the real solution, i.e., that $\ell + 1 < k$. This constraint is met for $r = 2$, when $n = n_2 = 35$, $k = k_2 = 14$, and $\ell = 11$. For $r \geq 6$, the constraint follows from

$$(\ell+1)/n = 1/3 + 1/3n < 0.41 < \sqrt{2} - 1 + \frac{4(3-2\sqrt{2})e_2^r - 4}{(4+3\sqrt{2})e_1^r + (4-3\sqrt{2})e_2^r} = \frac{k}{n}\,. \qquad \square$$

Remark: The vectors given in Theorem 5.7 have $n = 35,\ 40389, \ldots,$ where each value of n is about 577 times as great as the previous value. The example with $n = 35$ can be found in the computer-generated list of folded vectors with positive gap.

6. Computer-Generated Vectors with Positive Gap

For any given $n \in \mathbf{N}$ we can, in principle, apply Theorem 2.1 to all $2^{n+1} - 2$ vectors $a \in A_n$ to find those with positive gap. It is more efficient, however, to do our exhaustive search over *folded* vectors, of which there are only about $3^{n/2}$. The unfolded vectors corresponding to folded vectors with positive gap can then be examined individually to find those with gap of two, three, or more.

The search over folded vectors can itself be simplified considerably by making use of the superincreasing nature of the sequence of binomial coefficients $\binom{n}{j}$ for sufficiently small j, much as in Theorem 2.5. This is illustrated by the adaptive algorithm below, for odd n. A similar algorithm works for even n.

Algorithm 6.1: Suppose that n is odd. We seek all vectors $b = (b_0, \ldots, b_{(n-1)/2}) \in \{-1, 0, 1\}^{(n+1)/2}$ such that (3.2) holds.

We choose the components in reverse order, beginning with $b_{(n-1)/2}$, which multiplies the largest binomial coefficient in the sum. After choosing each new component b_k, we observe that

$$\sum_{0\le j\le (n-1)/2} (-1)^j \binom{n}{j} b_j = 0 \iff \sum_{k\le j\le (n-1)/2} (-1)^j\, b_j \binom{n}{j} = -\sum_{0\le j<k} (-1)^j\, b_j \binom{n}{j}$$

$$\implies \left|\sum_{k\le j\le (n-1)/2} (-1)^j\, b_j \binom{n}{j}\right| \le \sum_{0\le j<k} \binom{n}{j}.$$

If the last inequality is violated, then our choice of $(b_k, \ldots, b_{(n-1)/2})$ is inconsistent, so we can prune 3^k vectors from the search tree and try a different value of b_k. The search ends when we have either pruned or explicitly tried all $3^{(n+1)/2}$ vectors $b \in \{-1,0,1\}^{(n+1)/2}$.

The algorithm above requires about $2^{n/4}$ steps to test all $b \in B_n$. A Fortran implementation running for a week stealing unused machine cycles on a 4-processor 33-Megahertz MIPS R3000 system found all folded vectors with positive gap for $2 \le n \le 128$. In addition to the 98 solutions given in the theorems of Sections 3, 4, and 5, there are 21 essentially different new solution vectors, which we call “sporadic” because we do not know how to fit them into a family, plus 8 other solutions that can be written as simple linear combinations of the regular solutions, sporadic solutions, and easily explained virtual solutions. Each of these virtual solutions has either two or three nonzero components and corresponds to a Diophantine equation of first or second order.

In Table 2 we list all folded vectors with positive gap for $2 \le n \le 128$. To save space, we omit the 63 all-zero vectors, which are solutions for all odd n. We also omit the 21 vectors $(0,\ldots,0,2,1,0,\ldots,0)$, which occur for all n of the form $6t+2$. Thus of the 98 familiar solutions, only 14 are recorded in the table.

For even n, the components are written in the order $b_0, b_1, \ldots, b_{(n-2)/2}$. For odd n, we represent -1 and $+1$ by “$-$” and “$+$”, respectively. If $b \in B_n$ for odd n, then $-b \in B_n$ has the same gap, as discussed in Observation 3.3. We list just one of the two in the table.

After each vector given by a previous theorem we write “T” followed by the theorem number. If the vector is sporadic, we write S1, S2, or S3 to indicate that it is the first, second, or third essentially different sporadic solution for that value of n. If the vector can be expressed as a simple linear combination of “T” and “S” vectors, then the relevant theorem numbers and “sporadic solution” numbers are given. Finally, if virtual solutions

n		
13	0 0 0 + + − −	(T3.9)
14	0 0 0 0 1 2 1	(T3.7)
24	2 2 2 1 0 2 2 1 2 1 0 0	(S1)
	0 0 2 0 0 1 2 1 0 1 2 1	(S2)
29	0 0 0 0 0 0 0 − − 0 + − − 0 0	(S1)
31	0 0 0 − − 0 0 + − 0 − − + + − −	(S1)
	0 0 0 + + 0 0 − + + 0 + 0 + 0 −	(S2)
33	0 0 0 0 0 0 0 0 0 0 0 + + − − 0	(T3.9)
34	0 0 0 0 0 0 0 0 0 0 0 0 0 1 2 1 0	(T3.7)
	0 0 0 0 0 0 2 2 0 1 2 1 1 2 1 0 0	(S1)
	0 0 0 0 0 0 2 2 0 1 0 2 2 2 1 0 0	(S1,V1)
	0 0 0 0 0 0 2 2 0 1 2 1 1 0 1 1 0	(S1,V2)
	0 0 0 0 0 0 2 2 0 1 0 2 2 0 1 1 0	(S1,V1,V2)
35	+ + + + + + + + + + + + + + − − 0 0	(T5.4)
	+ + + + + + + + + + + − 0 + − − 0 0	(T5.7)
38	0 0 0 2 0 1 0 2 2 0 0 0 1 1 0 2 0 0 1	(S1)
41	0 0 0 0 0 + 0 + 0 0 0 + + − − − 0 − − 0 0	(S1)
	0 0 0 0 0 + 0 + 0 0 0 + + + 0 − 0 − − 0 0	(S1,V1)
	0 0 0 0 0 − − − + − 0 + 0 − 0 + − − 0 0 0	(S2)
	0 0 0 0 0 − − − + − 0 + 0 + + + − − 0 0 0	(S2,V1)
44	0 0 0 0 0 2 1 2 0 0 2 0 0 2 1 2 0 1 1 1 2 1	(S1)
47	0 0 0 0 0 0 0 0 0 0 0 + 0 0 + 0 + − − 0 0 0 0 0	(S1)
48	2 2 2 1 0 2 1 1 1 0 0 1 1 2 1 1 0 1 0 1 1 0 0 0	(S1)
54	0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 2 0 1 0 0 1 2 1 0 0 0 0	(S1)
61	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 + + − − 0 0	(T3.9)
62	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 2 1 0 0	(T3.7)
	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 2 1 0 0 0 0 1 2 1 0 0	(T5.5)
	0 0 0 0 2 2 0 0 0 0 1 1 0 2 1 0 2 0 1 1 0 1 2 0 1 2 1 0 1 1 0	(S1)
	0 0 0 0 2 2 0 0 0 0 1 1 0 2 1 0 2 0 1 1 2 2 2 0 1 2 1 0 1 1 0	(S1,T3.5)
	0 0 0 0 2 2 0 0 0 0 1 1 0 2 1 0 2 0 1 1 2 2 2 0 1 2 2 2 2 1 0	(S1,T3.5,T3.7)
	0 0 0 0 2 2 0 0 0 0 1 1 0 2 1 0 2 0 1 1 0 1 2 0 1 2 2 2 2 1 0	(S1,T3.7)
	0 0 0 0 2 2 0 0 0 0 0 1 2 1 2 1 0 2 2 0 2 0 1 2 0 2 2 0 1 1 0	(S2)
63	− − − − − + + 0 − 0 + 0 + + + + + 0 + + − + + + − − + + − − 0 0	(S1)
73	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 + 0 + − + 0 0 − 0 + 0 − 0 + − − 0 0 0 0 0 0	(S1)
	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 + 0 − 0 0 + − + − − 0 + + + − − 0 0 0 0 0 0	(S2)
74	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 2 1 0 2 0 2 2 2 1 1 1 1 2 1 0 0 0 0 0 0 0	(S1)
	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 2 0 1 2 1 1 2 2 1 1 2 1 0 0 0 0 0 0	(S2)
	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 2 1 2 2 2 1 1 2 2 1 1 2 1 0 0 0 0 0 0	(S3)
97	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 + + − − 0 0 0	(T3.9)
98	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 2 1 0 0 0	(T3.7)
	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 2 1 0 0 0 0 0 0 0 0 0 1 2 1 0 0 0	(T5.5)
103	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 + − − 0 0 0 0 0 0 0 0 0 0 0	(T3.8)
104	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 2 1 0 0 0 0 0 0 0 0 0 0 0	(T5.1)

Table 2:
Folded vectors with positive gap

are included in the linear combination, their presence is indicated by the notation V1, V2, etc., where V1 and V2 represent the first and second virtual solutions for that n.

In Table 3, we list $\Gamma(n)$ for $2 \le n \le 128$. To see how those values were obtained, first note that all lower bounds follow from Tables 1 or 2. As to the upper bounds, we know that $\gamma(a) \ge 1$ if and only if either a or its complement yields a folded vector in Table 2, or (for n odd) yields the zero vector, or (for $n = 6t+2$) yields the folded vector of Theorem 3.5. This reduces our task to a certain number of cases, which we now examine. So let $2 \le n \le 128$.

If n is odd, the only solutions $a \in A_n$ with $\gamma(a) \ge 2$ and a symmetric (so that $\varphi(a) = (0, \ldots, 0)$) are those given by Theorems 4.1 and 4.2. (Each vector can also be complemented.)

Similarly, for n even, the only solutions $a \in A_n$ with $\gamma(a) \ge 2$ for which the prefix vector πa is symmetric (and thus $\varphi(\pi a) = (0, \ldots, 0)$) are those given by Theorems 4.1 and 4.2. (These solutions can also be complemented and/or reversed.)

If there exists any other vector $a \in A_n$ with $\gamma(a) \ge 2$, then it follows by Theorem 2.3 that $\varphi(a)$ and $\varphi(\pi a)$ are folded vectors listed in Table 2 or given by Theorem 3.5 (possibly after complementation and/or reversal). Thus we may restrict attention to values of n for which both n and $n-1$ have representatives in Table 2 or are of the form $6t+2$; i.e., we consider

$$n \in \{14, 32, 33, 34, 35, 48, 62, 63, 74, 98, 104\}.$$

Of these, the zero entries for $n = 12, 60, 96, 102$ prove the claimed upper bounds for $n = 14, 62, 63, 98, 104$, by Theorem 2.3 (v). Thus to prove correctness of all entries of Table 3, it is sufficient to show $\Gamma(n) \le 1$ for $n = 32, 33, 48, 74$. These four cases have to be checked individually; we illustrate the analysis only for $n = 48$.

Lemma 6.2: $\Gamma(48) = 1$.

Proof: From Table 2 we see that there is exactly one folded vector in B_{48} with positive gap, namely

$$b = (b_0, \ldots, b_{23}) = (2,2,2,1,0,2,1,1,1,0,0,1,1,2,1,1,0,1,0,1,1,0,0,0) \ .$$

n	$\Gamma(n)$	n	$\Gamma(n)$	n	$\Gamma(n)$	n	$\Gamma(n)$
1	0	33	1	65	1	97	1
2	0	34	2	66	0	98	2
3	1	35	3	67	1	99	3
4	0	36	0	68	1	100	0
5	1	37	1	69	1	101	1
6	0	38	1	70	0	102	0
7	1	39	1	71	1	103	1
8	1	40	0	72	0	104	2
9	1	41	1	73	1	105	3
10	0	42	0	74	1	106	0
11	1	43	1	75	1	107	1
12	0	44	1	76	0	108	0
13	1	45	1	77	1	109	1
14	2	46	0	78	0	110	1
15	3	47	1	79	1	111	1
16	0	48	1	80	1	112	0
17	1	49	1	81	1	113	1
18	0	50	1	82	0	114	0
19	1	51	1	83	1	115	1
20	1	52	0	84	0	116	1
21	1	53	1	85	1	117	1
22	0	54	1	86	1	118	0
23	1	55	1	87	1	119	1
24	1	56	1	88	0	120	0
25	1	57	1	89	1	121	1
26	1	58	0	90	0	122	1
27	1	59	1	91	1	123	1
28	0	60	0	92	1	124	0
29	1	61	1	93	1	125	1
30	0	62	2	94	0	126	0
31	1	63	3	95	1	127	1
32	1	64	0	96	0	128	1

Table 3:
Maximal gaps for $n \leq 128$

Thus $\Gamma(48) \geq 1$. Neither 48 nor 47 is of the form $6t+2$, so if $\Gamma(48) \geq 2$, then there exists a vector $a = (a_0, \ldots, a_{48}) \in A_{48}$ such that $\varphi(a) = b$ and such that the prefix vector $\pi a = (a_0, \ldots, a_{47})$ has positive gap and is represented in Theorem 2.6 or in Table 2 for $n = 47$. Letting $b' = \varphi(\pi a)$, we see from Table 2 that this can happen only if

$$\begin{aligned} b' \in \{\ &(0,0,0,0,0,0,0,0,0,0,0,1,0,0,1,0,1,-1,-1,0,0,0,0,0),\\ &(0,0,0,0,0,0,0,0,0,0,0,-1,0,0,-1,0,-1,1,1,0,0,0,0,0),\\ &(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)\ \}. \end{aligned}$$

We may assume without loss of generality that $a_{24} = 0$. (If not, we just complement each bit in a.) Examining b, we have

$$\begin{aligned} a_4 + a_{44} = b_4 = 0 &\Longrightarrow a_4 = 0,\ a_{44} = 0;\\ a_5 + a_{43} = b_5 = 2 &\Longrightarrow a_5 = 1, a_{43} = 1. \end{aligned}$$

Thus $a_4 - a_{43} = -1$.

By examining b', however, we see that $a_4 - a_{43} = 0$ for all three possible values of b'. This contradiction shows that there is no vector $a \in A_{48}$ with $\gamma(a) \geq 2$. $\square$

Combining our previous results, we now list $\Gamma(n)$ for $n \leq 128$.

Theorem 6.3: *For $2 \leq n \leq 128$, the value of the maximal gap $\Gamma(n)$ is as given in Table 3. In particular,*

$$\max_{2 \leq n \leq 128} \Gamma(n) = 3. \qquad \square$$

The results for $n \leq 128$, together with heuristic probabilistic arguments based on the distribution of binomial coefficients, suggest that $\Gamma(n)$ might never exceed 3. Although this conjecture seems beyond the reach of our methods, we shall see in Section 7 that $\Gamma(n) = o(n)$ and that $\Gamma(n) \leq 3$ for all $n \leq \{500\}$.

7. Upper Bounds on the Gap

The numerical evidence of the previous section and heuristic probabilistic arguments indicate that the simple bound $\Gamma(n) < n/2$ is very loose. We now show that in fact $\Gamma(n) = O(n^{.548})$.

Theorem 7.1: *If $n+1$ is prime, then $\Gamma(n) = 0$.*

Proof: By Theorem 2.1, $\Gamma(n) > 0$ if and only if

$$\sum_{0 \le j \le n} (-1)^j \binom{n}{j} a_j = 0 \tag{7.1}$$

for some $a \in A_n$. Writing $p = n+1$ and using the fact that

$$\binom{p-1}{j} \equiv \frac{(-1)(-2)\cdots(-j)}{1 \cdot 2 \cdots j} \equiv (-1)^j \bmod p$$

for $0 < j < p$, we obtain

$$\sum_{0 \le j < p} (-1)^j \binom{p-1}{j} a_j \equiv \sum_{0 \le j < p} 1 \cdot a_j \bmod p.$$

This is congruent to $0 \bmod p$ only if the a_j's are all 0 or all 1. Since these two cases are excluded (they give trivial, constant, interpolating polynomials), (7.1) cannot be satisfied. Thus $\Gamma(n) = 0$. □

Together with Theorem 7.1, any upper bound on the gaps between consecutive prime numbers gives an upper bound on Γ.

Theorem 7.2: $\Gamma(n) = O(n^{.548})$.

Proof: From Theorems 7.1 and 2.1 it follows that $\Gamma(n) \le n - (p-1)$, where p is the largest prime less than or equal to $n+1$. By Mozzochi's (1986) theorem on prime number gaps, we have $p \ge n - O(n^{.548})$, and thus $\Gamma(n) = O(n^{.548})$. □

The table of prime numbers gives $m = \max\{\Gamma(n) : 1 \le n \le 128\} \le 13$, while the true value is $m = 3$, by Theorem 6.3.

We have obtained useful bounds on $\Gamma(n)$ for all n by considering (2.1) modulo p for an appropriate prime p. Using other primes between $n/2$ and n, we can check whether $\Gamma(n)$ continues to be bounded above by 3 for larger n. If $n, j, p \in \mathbf{N}$ with p prime, $n/2 < p \le n$, and $n - p < j < p$, then

$$\binom{n}{j} \equiv 0 \bmod p, \tag{7.2}$$

since p divides $n!$ and neither $j!$ nor $(n-j)!$. This leads to the following algorithm for finding all $a \in A_n$ with $\gamma(a) \geq 3$ for $n \leq \{500\}$.

Suppose that $\gamma(a) \geq 3$ for some $a \in A_n$. Then by Corollary 2.4,

$$\sum_{0 \leq j \leq n-2} (-1)^j \binom{n-2}{j} a_{j+i} = 0 \quad \text{for} \quad i \in \{0, 1, 2\}. \tag{7.3}$$

For given n, let p_1 be the largest prime less than or equal to n. For $k \geq 2$, let p_k be the largest prime less than p_{k-1}. We consider (7.3) modulo p_k for $k = 1, 2, \ldots,$ continuing until $p_k \approx n/2$.

Working modulo p_1 and applying (7.2) to (7.3), we obtain three constraints on the values of $a_0, \ldots, a_{n-p_1}$ and $a_{p_1}, \ldots, a_n$. (All other a_j's have coefficients divisible by p_1 in (7.3).) For moderate values of n, only a few values of $(a_0, \ldots, a_{n-p_1}, a_{p_1}, \ldots, a_n)$ satisfy all three constraints.

Next we consider (7.3) modulo p_2 to find three constraints on $(a_0, \ldots, a_{n-p_2}, a_{p_2}, \ldots, a_n)$. Thus for each solution $(a_0, \ldots, a_{n-p_1}, a_{p_1}, \ldots, a_n)$ from the previous step, we need only find which values of $(a_{n-p_1+1}, \ldots, a_{n-p_2}, a_{p_2}, \ldots, a_{p_1-1})$ are consistent with this earlier solution.

As long as the gaps between successive primes are sufficiently small, the number of admissible values of $(a_0, \ldots, a_{n-p_k}, a_{p_k}, \ldots, a_n)$ remains small for each k, and we can build up a incrementally.

By using a few simple tricks to reduce the complexity of the algorithm, we were able to find all vectors $a \in A_n$ with $n \leq \{500\}$ for which $\gamma(a) \geq 3$. The results are given in the following theorem.

8. Summary and Open Problems

We have investigated the minimal degree of nonconstant polynomials $f \in \mathbf{R}[x]$ that take only two values on the domain $\{0, 1, \ldots, n\}$. For each n, only a small fraction of the $2^{n+1} - 2$ nontrivial choices for $a = (f(0), f(1), \ldots, f(n))$ yield interpolating polynomials of degree less than n. We have found several infinite families of vectors a for which the gap $\gamma(a) = n - \deg(f)$ is positive. These solutions can all be derived from first- or second-order Diophantine equations together with the standard binomial identities.

We have also identified by computer search all such solutions with $n \leq 128$ and have found that the maximal gap $\Gamma(n)$ never exceeds 3 for these values of n. Another computer search revealed that $\Gamma(n)$ is at most 3 for all $n \leq \{500\}$.

Theorems 7.1 and 7.2 show that $\Gamma(n) = 0$ whenever $n+1$ is prime and that for general n, $\Gamma(n) = O(n^{.548})$. Szegedy observed that can apply the results of Nisan and Szegedy (1992) to obtain the following.

Theorem 8.1: *Let $g\colon \{0,1\}^n \to \{0,1\}$ be a nonconstant symmetric Boolean function of n variables, d its Fourier degree, and $a = (a_0, \ldots, a_n) \in A_n$ with $a_i = g(1^i 0^{n-i})$ for $0 \leq i \leq n$. Then $d = n - \gamma(a)$, and hence*

$$n - O(n^{.548}) \leq n - \Gamma(n) \leq d \leq n.$$

The central question of this paper remains open:

Question 1: What is the order of $\Gamma(n)$?

Remark: Heuristic arguments based on the distribution of binomial coefficients, bolstered by numerical evidence, indicate that $\Gamma(n) = O(1)$, perhaps with $\Gamma(n) \leq 3$ for all n.

Question 2: If $f(0), \ldots, f(n)$ are in $\{0, 1, \ldots, k-1\}$ with the $f(j)$'s not all equal, what bounds can we give on $\Gamma_k(n) = \max\limits_{f(0),\ldots,f(n)} \{n - \deg(f)\}$?

Remark: For all $k \geq 2$, the bound $\Gamma_k(n) < \frac{k-1}{k}\, n$ is trivial, but the techniques of this paper do not yield a sublinear bound on the gap $\Gamma_k(n)$ for $k \geq 3$. Heuristic arguments based on the distribution of binomial coefficients suggest, however, that for each k there is a constant C_k such that $\Gamma_k(n) \leq C_k$ for all n. It may be possible using analytic methods to show that for any given $k \geq 2$, $\Gamma(n) = O(n^{\frac{1}{2}+\epsilon})$ for arbitrarily small $\epsilon > 0$.

Some results of this paper are valid more generally than stated; for example, the characterizations of Section 2 obviously hold for fields of characteristic zero or $p > n$. Theorem 7.1 then implies that every two-valued polynomial of degree less than p over a finite prime field $\mathbf{F}_p$ has maximal degree, namely $p-1$. The trace from $\mathbf{F}_{2^n}$ to $\mathbf{F}_2$ shows that this is not true for all finite fields.

Question 3: Which degrees less than $q-1$ can two-valued polynomials over a finite field $\mathbf{F}_q$ have?

Acknowledgements

Thanks go to Andrew Odlyzko for providing the reference on the difference between consecutive primes. Special thanks go to Mario Szegedy, who posed the problem considered in this paper and who greeted our results with gratifying enthusiasm. He also noted Theorem 8.1.

The first author gratefully acknowledges the hospitality of Gaston Gonnet at ETH Zürich, Switzerland, where part of this work was done. It was partially supported by the Natural Sciences and Engineering Research Council of Canada, and the Information Technology Research Centre, Ontario.

References

[1] C. J. Mozzochi, "On the difference between consecutive primes," *J. Number Theory* **24** (1986), 181–187.

[2] N. Nisan and M. Szegedy, "On the degree of Boolean functions as real polynomials," *STOC* 1992, Victoria, 462–474.

[3] D. Singmaster, "Repeated binomial coefficients and Fibonacci numbers," *The Fibonacci Quarterly* **13** (1975), 295–298.

[4] C. A. Tovey, "Multiple occurrences of binomial coefficients," *The Fibonacci Quarterly* **23** (1985), 356–358.

Polynomials with Two Values

Joachim von zur Gathen

AT&T Bell Laboratories
Department of Computer Science, University of Toronto
Toronto, Ontario, Canada M5S 1A4

James R. Roche

AT& T Bell Laboratories
Murray Hill, New Jersey 07974

ABSTRACT

This paper investigates the minimal degree of polynomials $f \in \mathbf{R}[x]$ that take only two values on a given range of integers $\{0, \ldots, n\}$. We show that the *gap*, defined as $n - \deg(f)$, is $O(n^{.548})$. The maximal gap for $n \leq 128$ is 3. As an application, we obtain a bound on the Fourier degree of symmetric Boolean functions.