NULLSPACE-PRIMES AND FIBONACCI POLYNOMIALS

William F. Klostermeyer

Dept. of Computer and Information Sciences, University of North Florida, Jacksonville, FL 32224-2669

John L. Goldwasser

Dept. of Mathematics, West Virginia University, Morgantown, WV 26506

e-mail: klostermeyer@hotmail.com; jgoldwas@math.wvu.edu

(Submitted July 2000-Final Revision August 2001)

1. INTRODUCTION

A nonzero $m \times n$ $(0, 1)$-matrix A is called a *nullspace matrix* if each entry (i, j) of A has an even number of 1's in the set of entries consisting of (i, j) and its rectilinear neighbors. It is called a nullspace matrix since the existence of an $m \times n$ nullspace matrix implies the closed neighborhood matrix of the $m \times n$ grid graph is singular over $GF(2)$. By *closed neighborhood matrix,* we mean the adjacency matrix of the graphs with 1's down the diagonal.

In Sections 2 and 3, we review the relationship of the Fibonacci polynomials to nullspace matrices. In Section 3, we define *composite* and *prime* nullspace matrices and present some number sequences related to the nullspace matrices and pose a question analogous to the famous question about whether or not there exist infinitely many prime Fibonacci numbers.

2. BACKGROUND

In this paper, all polynomials are over the binary field $GF(2)$. When no confusion results, we denote the all-zero n-vector simply by 0. See Table 1 for an example of a nullspace matrix.

TABLE 1. A 4×4 Nullspace Matrix

1	0	0	0
1	1	0	0
1	0	1	0
0	1	1	1

If we choose a nonzero vector $w \in F^n$, where F^n is the binary *n-tuple* space and let w be the first row of a matrix A, for each $i > 1$ there is a unique way to choose the i^{th} row to make the number of 1's in the closed neighborhood of each entry in the $(i-1)^{\text{st}}$ row even. If r_i is the i^{th} row, the unique way of doing this is given by

$$r_i = Br_{i-1} + r_{i-2},\ i \geq 2,\ r_0 = 0, r_1 = w, \tag{1}$$

where $B = [b_{ij}]$ is the $n \times n$ tridiagonal $(0, 1)$-matrix with $b_{ij} = 1$ if and only if $|i - j| \leq 1$ (and the r_i's in (1) are written as column vectors). If $r_{m+1} = 0$ for some positive integer m, then $r_1, r_2, \ldots, r_m$ are the rows of an $m \times n$ nullspace matrix. We can also compute the entries of r_i one at a time by $r_i[j] = r_{i-1}[j] + r_{i-1}[j-1] + r_{i-1}[j+1] + r_{i-2}[j] \bmod 2$.

It follows from the definitions that $r_i = f_i(B)w$ for $i = 0, 1, 2, \ldots$, where f_i is the i^{th} Fibonacci polynomial over $GF(2)$:

$$f_i = xf_{i-1} + f_{i-2},\ i \geq 2,\ f_0 = 0, f_1 = 1. \tag{2}$$

In this paper, we are interested in building large nullspace matrices from smaller ones. A fundamental property of nullspace matrices is given in the following simple proposition.

Proposition 1: Let n and k be positive integers with $k+1$ a multiple of $n+1$. If there exists an $n \times n$ nullspace matrix, then there also exists a $k \times k$ nullspace matrix.

To see this another way, if $k+1 = q(n+1)$ where q is a positive integer, and if A is an $n \times n$ nullspace matrix, then a $k \times k$ nullspace matrix can be constructed by letting row and column numbers $n+1$, $2(n+1), \ldots, (q-1)(n+1)$ have all entries equal to zero, creating a $q \times q$ array of $n \times n$ squares, putting A in one of the $n \times n$ squares and filling in the rest of them by "reflecting" across the lines of zeros. That is, one can take the 4×4 nullspace matrix from Table 1 and construct a 9×9 nullspace matrix; see Table 2.

TABLE 2. A 9×9 Nullspace Matrix

1	0	0	0	0	0	0	0	1
1	1	0	0	0	0	0	1	1
1	0	1	0	0	0	1	0	1
0	1	1	1	0	1	1	1	0
0	0	0	0	0	0	0	0	0
0	1	1	1	0	1	1	1	0
1	0	1	0	0	0	1	0	1
1	1	0	0	0	0	0	1	1
1	0	0	0	0	0	0	0	1

3. NULLSPACE-PRIMES

We call a nullspace matrix that has at least one row or column of zeros a *composite nullspace matrix*, otherwise we say it is a *prime nullspace matrix*. We say that an integer n is *nullspace-prime* if there exists an $(n-1) \times (n-1)$ nullspace matrix, but for no proper divisor m of n does there exist an $(m-1) \times (m-1)$ nullspace matrix. With the aid of a computer, we have determined that the first few nullspace-primes are 5, 6, 17, 31, 33, 63, 127, 129, 171, 257, 511, 683. This sequence does not match any in *Sloane's Encyclopedia of Integer Sequences*. Other nullspace-primes include 2047, 2731, 2979, 3277, 3641, and 8191. We prove below that 6 is, in fact, the only even nullspace-prime. It is easy to see that there exists an $n \times n$ nullspace matrix if and only if n is one less than a multiple of a nullspace-prime.

One could use a simple (albeit, rather slow) sieving algorithm to determine if an integer n is a nullspace-prime, assuming we know that there exists an $(n-1) \times (n-1)$ nullspace matrix (which can be determined in $O(n \log^2 n)$ time [1]). For example, 693 is not a nullspace-prime since 693 modulo $33 = 0$, though there does exist a 692×692 nullspace matrix.

We say two polynomials $p_1(x)$ and $p_2(x)$ are *conjugates* if $p_1(x+1) = p(x)$. If $p(x)$ is an irreducible polynomial, we say that the *Fibonacci index* of $p(x)$ is t if t is the smallest positive integer such that $p(x)$ divides $f_t(x)$. The following is from [1].

Theorem 2 [1]: There exists an $n \times m$ nullspace matrix if and only if $f_{n+1}(x)$ and $f_{m+1}(x+1)$ are not relatively prime.

Theorem 2 is a special case of the following result (letting $r = 0$ in Proposition 3 below yields Theorem 2), also from [1].

Proposition 3: Let X be the closed neighborhood matrix of the $m \times n$ grid graph. If r is the degree of the greatest common divisor of $f_{n+1}(x+1)$ and $f_{m+1}(x)$, then the fraction of $n \times 1$ 0-1 vectors z having solutions y to the equation $Xy - z$ is 2^{-r}.

Proposition 3 was proved using the Primary Decomposition Theorem for linear operators, also known as the Spectral Decomposition Theorem (cf. [4]).

To illustrate Theorem 2, there exists a 16×16 nullspace matrix because $f_{17}(x)$ has the self-conjugate irreducible factor and there exists a 32×32 nullspace matrix because $f_{33}(x)$ has the conjugate pair of irreducible factors $x^5 + x^4 + x^3 + x + 1$ and $x^5 + x^3 + x^2 + x + 1$.

Using Theorem 2, we can prove that there is only one even nullspace-prime.

Fact 4: The only even nullspace-prime is 6.

Proof: As there do not exist 1×1 or 3×3 nullspace matrices, 2 and 4 are not nullspace-primes. Let $n > 6$ be an even integer and suppose n were a nullspace-prime. Then there exists an $(n-1) \times (n-1)$ nullspace matrix. Hence, by Theorem 2, $f_n(x)$ and $f_n(x+1)$ have a common factor. It was shown in Lemma 4, part (3), of [1] (using induction), that $f_{2n} = xf_n^2$ for all $n \geq 0$. Lemma 4, part (5), of [1] states that $f_{mn}(x) = f_m(x) f_n(x f_m(x))$, for $m, n \geq 0$. It follows that either there exists an $(\frac{n}{2} - 1) \times (\frac{n}{2} - 1)$ nullspace matrix, in which case n is not a nullspace-prime, or that x and $x+1$ are a conjugate pair of factors of $f_n(x)$ and $f_n(x+1)$. Using Lemma 4 of [1] and induction, it is not hard to prove that $x+1$ is a factor of f_k if and only if $3|k$ and this property also happens to be a special case of Proposition 5(b) of [1]. Hence, we have that $6|n$, which implies that n is not a nullspace-prime. □

For completeness, we note that Proposition 5(b) from [1] states that, if $p(x)$ is an irreducible polynomial other than 1 or x with Fibonacci index t, then $p(x)|f_r(x)$ if and only if $t|r$. The proof of this property is based on Lemma 4 of [1].

We state a theorem from [3] that follows from results in [1]. Recall that B is the $n \times n$ tri-diagonal matrix defined in Section 2.

Theorem 5 [3]: The set of all vectors w that can be the first row of an $m \times n$ nullspace matrix is equal to the nullspace N_{m+1} of $f_{m+1}(B)$. If $d_{m+1}(x)$ is the greatest common divisor of $f_{n+1}(x+1)$ and $f_{m+1}(x)$, then the nullspace of $d_{m+1}(B)$ is equal to N_{m+1} and has dimension equal to the degree of d_{m+1}.

As can be concluded from the results in [1] and [3], if an $m \times n$ nullspace matrix has a row of zeros and if the first such row is the $(j+1)^{\text{st}}$, then $j+1$ divides $m+1$ and row r is all zeros if and only if r is a multiple of $j+1$. The same is true of columns (with n in place of m), since a matrix is a nullspace matrix if and only if its transpose is.

As we noted above, 63 is a nullspace-prime, so there is no way to "piece together" square nullspace matrices to get a 62×62 nullspace matrix. But there does exist a 6×8 nullspace matrix. A 9×7 array of this nullspace matrix and its reflections, with rows and columns of zeros in between, can be used to construct a composite 62×62 nullspace matrix. Therefore, if n is a nullspace-prime, there may exist an $(n-1) \times (n-1)$ composite nullspace matrix. But it is not hard to show that there must also exist an $(n-1)\times(n-1)$ prime nullspace matrix (the sum of the 62×62 composite nullspace matrix and its 90 degree rotation is a prime nullspace matrix). This situation, and more, is described in the following theorem; an example is given following the proof of the theorem.

Theorem 6: Let n be an even positive integer and let $d_{n+1}(x)$ have positive degree and be the greatest common divisor of $f_{n+1}(x)$ and $f_{n+1}(x+1)$. Then:

(1) Every $n\times n$ nullspace matrix is prime if and only if every irreducible factor of $d_{n+1}(x)$ has Fibonacci index equal to $n+1$.

(2) Every $n\times n$ nullspace matrix is composite if and only if $d_{n+1}(x)$ divides $f_{t+1}(x)$ for some $t+1\neq 0$ less than $n+1$.

Proof: Let $p_1, p_2, \ldots, p_k$ be the irreducible factors of d_{n+1}, and let W_i be the nullspace of $p_i(B)$ for $i=1,2,\ldots,k$, where B is the tridiagonal matrix defined above. We note that the W_i intersection $W_j=\{0\}$ for $i\neq j$, and that each W_i is invariant under multiplication by B ($B\alpha_i\in W_i$ for each $\alpha_i\in W_i$). So the nullspace of $d_{n+1}(B)$ is equal to the direct sum $W_1\oplus W_2\oplus\cdots\oplus W_k$. By Theorem 5, this is equal to the set of vectors that can be the first row of an $n\times n$ nullspace matrix. Choose a nonzero vector $\alpha_i\in W_i$ for each i. Let f be any polynomial. Then $f(B)(\alpha_1+\alpha_2+\cdots\alpha_k)=0$ if and only if $f(B)\alpha_i=0$ for each i, and this happens if and only if f is divisible by p_i for each i. If some p_i has Fibonacci index $t+1$ where $t\leq n$, then every nonzero vector in W_i is the first row of an $n\times n$ nullspace matrix with $(t+1)^{\text{st}}$ row all zeros. If there is no such t, then each $n\times n$ nullspace matrix is prime, establishing (1).

Letting the polynomial f above be d_{n+1}, it is clear that if d_{n+1} divides f_{t+1} for some $t\neq 0$ less than n, then every $n\times n$ nullspace matrix has $(t+1)^{\text{st}}$ row all zeros. And if there is no such t, then the vector $\alpha_1+\alpha_2+\cdots+\alpha_k$, where α_i is a nonzero vector in W_i for each i, is the first row of a prime $n\times n$ nullspace matrix. □

For example, every 32×32 nullspace matrix is prime because

$$d_{33}(x)=(x^5+x^4+x^3+x+1)^2(x^5+x^3+x^2+x+1)^2$$

and each of these factors has Fibonacci index 33. But no 98×98 nullspace matrix is prime because $d_{99}(x)=d_{33}(x)$. Every 98×98 nullspace matrix has row and column numbers 33 and 66 with all entries zero.

Corollary 7: If $n+1$ is a prime number, then there exists no $n\times n$ composite nullspace matrix.

We now pose our main open question.

Question 1: Are there an infinite number of nullspace-primes?

One might also ask whether or not a polynomial time algorithm exists to determine if an integer is nullspace-prime or not.

What more can be said about the distribution of nullspace-primes? From the few listed above, we can see that many take the form $2^k\pm 1$, but there are many nullspace primes that are not of this form; being of this form does not guarantee being nullspace-prime, take for example 65. In general, Fibonacci polynomials of the form $f_{2^k+1}(x)$ and $f_{2^k-1}(x)$ have many distinct factors [3], as do those with indices that are of the form $(2^k\pm 1)/p$, where p is a "small" prime. For example,

f_{171} has eleven distinct nontrivial factors and f_{683} has 31 distinct nontrivial factors. Thus, it is not surprising, given the results from [3], that many of these indices turn out to be nullspace-primes. What is not fully understood is how to characterize more precisely when an integer if nullspace-prime, even if it is of the form $2^k \pm 1$.

4. SUPER NULLSPACE-PRIMES

Define n to be *super nullspace-prime* if there exists no $(n-1)\times(n-1)$ composite nullspace matrix and there exists an $(n-1)\times(n-1)$ nullspace matrix. As mentioned above, 63 is nullspace-prime, but not super nullspace-prime. But 33 is super nullspace-prime because there does not exist a 2×10 nullspace matrix. Or, using Theorem 6(1), we see that

$$d_{33}(x) = (x^5+x^4+x^3+x+1)^2(x^5+x^3+x^2+x+1)^2$$

and each of these two factors has Fibonacci index 33. The integers 5, 6, 17, 31, 33, 127, 129, 171, 257, 511, 683 are super nullspace-prime. Of course, although 29 is prime, 29 is not nullspace-prime or super nullspace-prime since there does not exist a 28×28 nullspace matrix.

We know from [3] that, if $n=2^k$ where $k>3$, or $n=2^k-2$ where $k>3$, that there exists an $n\times n$ nullspace matrix. Thus, if n is prime and either $n-1=2^k$ or $n-1=2^k-2$, then $n+1$ is super nullspace-prime, such as $n=257$. But it seems likely that in order to determine whether an integer is super nullspace-prime requires factoring that integer or computing the Fibonacci indices of a number of polynomials, if we use the criteria described in Theorem 6(1), neither of which we know how to do efficiently (i.e., in polynomial time).

Conjecture 2: There are an infinite number of super nullspace-primes.

Note that, if the conjecture is false, then there are only finitely many Mersenne primes. We leave as an open problem determining how many *super nullspace composites* there are: integers, such as 99, which are such that there exists an $(n-1)\times(n-1)$ nullspace matrix and every $(n-1)\times(n-1)$ nullspace matrix is composite. Likewise, how many integers, such as 63, are nullspace-prime but not super nullspace-prime?

ACKNOWLEDGMENT

We thank the anonymous referee for a careful reading of the manuscript and for many valuable suggestions.

REFERENCES

1. J. Goldwasser, W. Klostermeyer, & G. Trapp. "Characterizing Switch-Setting Problems." *Linear and Multilinear Algebra* **43** (1997):121-35.
2. J. Goldwasser & W. Klostermeyer. "Maximization Versions of 'Lights Out' Games in Grids and Graphs." *Congressus Numerantium* **126** (1997):99-111.
3. J. Goldwasser, W. Klostermeyer, & H. Ware. "Fibonacci Polynomials and Parity Domination in Grid Graphs." Accepted for publication in *Graphs and Combinatorics*.
4. K. Hoffman & R. Kinze. *Linear Algebra*. Englewood Cliffs, NJ: Prentice Hall, 1971.

AMS Classification Numbers: 11T06, 12E05, 12E10, 05C99

❖❖❖