HAMMING DISTANCE FROM IRREDUCIBLE POLYNOMIALS OVER $\mathbb{F}_2$

GILBERT LEE, FRANK RUSKEY, AND AARON WILLIAMS

ABSTRACT. We study the Hamming distance from polynomials to classes of polynomials that share certain properties of irreducible polynomials. The results give insight into whether or not irreducible polynomials can be effectively modeled by these more general classes of polynomials. For example, we prove that the number of degree n polynomials of Hamming distance one from a randomly chosen set of $\lfloor 2^n/n \rfloor$ odd density polynomials is asymptotically $(1-e^{-4})2^{n-1}$, and this appears to be inconsistent with the numbers for irreducible polynomials. We also conjecture that there is a constant c such that every polynomial has Hamming distance at most c from an irreducible polynomial. Using exhaustive lists of irreducible polynomials over $\mathbb{F}_2$ for degrees $1 \le n \le 32$, we count the number of polynomials with a given Hamming distance to some irreducible polynomial of the same degree. Our work is based on this "empirical" study.

1. Introduction and Motivation

In this paper we are motivated by the following natural question: Under some appropriate measure how far can a polynomial be from being irreducible? We are mainly concerned with polynomials over the two element finite field and where the distance measure is the Hamming distance between polynomials of the same degree. Using recently computed exhaustive lists of irreducible polynomials up to degree 33, we compute the number of polynomials having a given Hamming distance from the set of irreducible polynomials. We conjecture that there is an absolute constant c such that every polynomial is of distance at most c from an irreducible polynomial. The data supports the conjecture that $c = 3$ for polynomials with non-zero constant term.

Let $\mathbb{F}_q$ denote the finite field with q elements. By $\mathbb{F}_q[z]$ we denote the set of monic polynomials with coefficients in $\mathbb{F}_q$. The Hamming distance $H(P(z), Q(z))$ between two polynomials $P(z) = \sum p_k z^k$ and $Q(z) = \sum q_k z^k$ is the number of coefficients for which $p_k \neq q_k$. Let $I_q(n,d)$ be the number of monic polynomials $P(z) \in \mathbb{F}_q[z]$ with non-zero constant term for which d is the smallest value such that there is a monic degree n irreducible polynomial $Q(z)$ with $d = H(P(z), Q(z))$. By $I(n,d)$ we mean $I_2(n,d)$.

A polynomial is irreducible if it cannot be factored into the product of two non-trivial polynomials. The number of monic irreducible polynomials over $\mathbb{F}_q$ is

$$\frac{1}{n}\sum_{d|n} \mu(d) q^{n/d} \sim \frac{1}{n} q^n. \tag{1}$$

Research supported in part by NSERC.

If a polynomial is irreducible over $\mathbb{F}_q$ then the sum of its coefficients is not divisible by q, because otherwise 1 would be a root. In particular over $\mathbb{F}_2$, the sum of the coefficients is odd.

Conventional wisdom suggests that the coefficients of irreducible polynomials are uniformly distributed in the limit, as n tends to infinity. A typical result is that of Uchiyama [9] stated below. This result was corrected by Hayes [5] (and extended by Cohen [3]).

Theorem 1.1 (Uchiyama/Hayes)**.** *The number of monic irreducible polynomials in $\mathbb{F}_q$ whose first s and last t (≥ 1) coefficients are fixed (with non-zero constant coefficient) is, for $\frac{1}{2} \leq v < 1$,*

$$\frac{q^n}{n(q-1)q^{s+t-1}} + O\left(\frac{q^{nv}}{n}\right).$$

With reference to (1), this is exactly what you would expect if the coefficients were distributed uniformly.

It is natural to investigate the distance question with sets of random polynomials to see if our experimental data support the hypothesis of uniformity. Surprisingly, we will see that this is not the case.

Two key properties of the set of irreducible polynomials over $\mathbb{F}_2$ are

- **Odd density:** In every irreducible polynomial the number of non-zero coefficients is odd. Otherwise, 1 is a root of the polynomial.
- **Reciprocal-closed:** The reciprocal of every irreducible polynomial is also irreducible. The reciprocal of a degree n polynomial $p(z)$ over $\mathbb{F}_2$ is the polynomial $z^n p(1/z)$.

The central question that we are trying to answer is: with respect to the Hamming distance question, are these properties (or just one of them) sufficient to explain the observed data? We believe that the answer is *no*. This is surprising since the only results known to us regarding the distribution of the coefficients of irreducible polynomials suggests that they behave in the limit like random polynomials.

Here is an outline of the paper. In Section 2 we show tables of our experimental results and briefly discuss the methodology used to produce them. Our results here allow us to extend a theorem of A. Bérczes and L. Hajdu [1]. In Section 3 we study the distance from random sets of binary strings with the odd density property. These results show consistent bias towards the data so in Section 4 we refine the model to also have the reverse-closed property (corresponds to the polynomials being reciprocal-closed). As we shall see, the refined model turns out to have the same asymptotics as the initial model.

2. Results for $\mathbb{F}_2$

We used the method described in [2] to produce tables of irreducible polynomials over $\mathbb{F}_2$. To compute the distance table we do a breadth-first search of the underlying graph of polynomials. Each polynomial of degree n is represented by a bitstring of length $n-1$. For example, the polynomial

$$x^{24}+x^{23}+x^{22}+x^{21}+x^{20}+x^{16}+x^{14}+x^{12}+x^{10}+x^{8}+x^{4}+x^{3}+x^{2}+x+1 \tag{2}$$

is represented as 11110001010101010001111. It is natural to use the bitstrings, interpreted as binary numbers, to index into an array that keeps track of the distance corresponding to that index. However, this would require far too much memory. We are forced to pack the information into computer words. We keep two arrays, one for polynomials of even distance, and the other for polynomials of odd distance, scanning one while updating the other.

The rightmost non-zero values in each row $1 \le n \le 17$ in Table 1 were previously computed in [1] (Table I., pg. 395), which contains the following theorem about irreducibility over the rationals.

Theorem 2.1. *If $0 \le n \le 22$, then for every monic polynomial $P \in \mathbb{Z}[x]$ of degree n there exists an irreducible monic polynomial $Q \in \mathbb{Z}[x]$ of degree n such that $|P-Q| \le 4$.*

Our results extend this Theorem to $0 \le n \le 32$.

Our calculations also show that there are polynomials at distance four from the set of *primitive* polynomials. There is 1 for $n = 24$ and 2 for $n = 32$, but no others in the range $1 \le n \le 32$.

3. Distance using a random set

Instead computing the Hamming distances from the set of irreducible polynomials, what happens when we compute Hamming distances to a random set of polynomials, each having an odd number of non-zero coefficients? It will be convenient restate our results in terms of bitstrings. We identify the bitstring $b_1b_2\cdots b_N$ with the polynomial $x^{N+1}+b_Nx^N+\cdots+b_1x+1$.

Let us first prove a technical lemma.

Lemma 3.1. *Let*

$$T(n) = \binom{2^n-p}{m} \Big/ \binom{2^n}{m}$$

where p and m are integers for which $p = O(n^k)$ (for some fixed k) and $m = o(2^n)$. Then

$$\ln T(n) = \ln\left(\left(1-\frac{m}{2^n}\right)^p\right) + O\left(\frac{p}{2^n-m}\right) + O\left(m\left(\frac{p}{2^n-m}\right)^2\right).$$

$n\backslash d$	0	1	2	3
1	1			
2	1	1		
3	2	2		
4	3	4	1	
5	6	8	2	
6	9	16	7	
7	18	32	14	
8	30	63	34	1
9	56	128	72	
10	99	255	157	1
11	186	510	326	2
12	335	1020	689	4
13	630	2032	1418	16
14	1161	4048	2935	48
15	2182	8109	6010	83
16	4080	16216	12304	168
17	7710	32434	25058	334
18	14532	64731	51004	805
19	27594	129597	103478	1475
20	52377	258718	209767	3426
21	99858	517424	424430	6864
22	190557	1034430	858019	14146
23	364722	2067780	1732430	29372
24	698870	4132038	3495434	62266
25	1342176	8262934	7046432	125674
26	2580795	16515320	14196421	261896
27	4971008	33021972	28583424	532460
28	9586395	66029987	57522469	1078877
29	18512790	132008983	115704938	2208745
30	35790267	263944002	232645189	4491454
31	69273666	527772375	467597246	9098537
32	134215680	1055126462	939526144	18615362

TABLE 1. The values of $I(n,d)$ for $1 \le n \le 32$.

Proof. By Taylor's expansion with remainder, for z approaching zero,

$$\ln(1-z) = -\sum_{k=1}^{q} \frac{z^k}{k} + O(z^{q+1}), \tag{3}$$

But we only need the case of $q = 1$ below. The following expansion for the Harmonic numbers is well-known (e.g., [8], pg. 278).

$$H(n) = \ln n + \gamma + O(1/n). \tag{4}$$

Note that

$$T(n) = \binom{2^n - p}{m} / \binom{2^n}{m} = \prod_{i=0}^{m-1} \frac{2^n - p - i}{2^n - i} = \prod_{i=0}^{m-1} \left(1 - \frac{p}{2^n - i}\right).$$

Now take logarithms, and apply (3) and (4).

$$\begin{aligned}
\ln T(n) &= \sum_{i=0}^{m-1} \ln\left(1 - \frac{p}{2^n - i}\right) \\
&= \sum_{i=0}^{m-1} \left(\frac{-p}{2^n - i} + O\left(\left(\frac{p}{2^n - i}\right)^2\right)\right) \\
&= -p\left(H(2^n) - H(2^n - m)\right) \ + \ O\left(m\left(\frac{p}{2^n - m}\right)^2\right) \\
&= -p\left(\ln(2^n) - \ln(2^n - m) + O(\frac{1}{2^n}) + O(\frac{1}{2^n - 2m})\right) \ + \ O\left(m\left(\frac{p}{2^n - m}\right)^2\right) \\
&= \ln\left(1 - \frac{m}{2^n}\right)^p + O\left(\frac{p}{2^n - m}\right) + O\left(m\left(\frac{p}{2^n - m}\right)^2\right)
\end{aligned}$$

□

3.1. **Hamming distances to an odd density set.** By $S(N,M)$ we denote a set of M odd density bitstrings each of length N, chosen uniformly at random from the set of all 2^N odd density bitstrings of length N. We say that a bitstring is *odd* if it has odd density; otherwise, it is *even*. The Hamming distance $H(b,c)$ between two bitstrings b and c of length N is the number of positions in which the corresponding bits differ. We say that two bitstrings are *adjacent* if their Hamming distance is one; i.e., they are adjacent in the hypercube. We extend the notation to sets S of bitstrings by defining $H(b,S) = \min\{H(b,s) \mid s \in S\}$.

Given a set of length N bitstrings S, the *neighborhood*, $\mathcal{N}(S)$, of S is the set $\{b \in \{0,1\}^N \mid H(b,s) = 1 \text{ for some } s \in S\}$; in other words it is exactly the same as the open neighborhood of S in the hypercube Q_N, in the graph theoretic sense.

Theorem 3.2. *Let S be a randomly chosen set of M odd bitstrings of length N and let b be some fixed bitstring of length N.*

$$Pr(H(b,S) \geq 2d+1 \mid b \ \textit{even}) = \binom{2^{N-1} - \sum_{j=0}^{d-1}\binom{N}{2j+1}}{M} / \binom{2^{N-1}}{M} \tag{5}$$

$$Pr(H(b,S) \geq 2d \mid b \ \textit{odd}) = \binom{2^{N-1} - \sum_{j=0}^{d-1}\binom{N}{2j}}{M} / \binom{2^{N-1}}{M} \tag{6}$$

FIGURE 1. The graph of $2^{-(N-1)}\mathcal{E}[|\mathcal{N}(S(N,M))|]$ for $n = 8, 16, 32, 64, 128, 256$. The horizontal axis shows $100m/2^{n-1}$.

Proof. There are a total of $\binom{2^{N-1}}{M}$ ways to select S. Suppose that b is even. We may assume that b consists solely of 0's, that is $b = 0^N$. In order for b to be distance $2d+1$ away from any string in S, the set S can have no bitstrings of density $1, 3, \ldots, 2d-1$. The number of such forbidden strings is $\binom{N}{1} + \binom{N}{3} + \cdots + \binom{N}{2d-1}$. The argument for b odd is similar and is omitted. □

Corollary 3.3. *The expected size of the set* $\{b \in 0, 1^N \mid H(b, S(N,M)) = d\}$ *is*

$$2^{N-1}\left(Pr(H(b,S) \geq d \mid b \not\equiv d \bmod 2) - Pr(H(b,S) \geq d+2 \mid b \not\equiv d \bmod 2)\right).$$

Proof. Follows directly from Theorem 3.2. □

In Figure 1 we show $2^{-(N-1)}\mathcal{E}[|\mathcal{N}(S(N,M))|]$ for selected values of N and varying M.

To make comparisons with irreducible polynomials over $\mathbb{F}_2$, we set $N = n-1$ and $m = 2^n/n$ (from (1)).

Theorem 3.4. *Asymptotically,* $\mathcal{E}[|\{b \in 0, 1^N \mid H(b, S(N,M)) = d\}|]$ *is equal to*

$$\begin{cases} 2^n/n & \text{if } d = 0 \\ 2^{n-1}(1-e^{-4}) & \text{if } d = 1 \\ 2^{n-1} - 2^n/n & \text{if } d = 2 \\ 2^{n-1}e^{-4} & \text{if } d = 3 \\ 0 & \text{if } d \geq 4. \end{cases}$$

Proof. The case $d = 0$ follows from (1). We explain the $d = 1$ case below, and leave the remaining for the full paper.

We substitute $N = n-1$ and $m = 2^n/n$ in Corollary 3.3 and then apply Lemma 3.1 to the binomial coefficient ratio $T(n) = \binom{2^{n-2}-n}{2^n/n} / \binom{2^{n-2}-n}{2^n/n}$.

$$\begin{aligned} \ln T(n) &= \ln\left(\left(1-\frac{2^n/n}{2^{n-2}}\right)^{n-1}\right) + O(\frac{n}{2^n}) \; + \; O\left(\frac{n^3}{2^{n-2}(n-4)^2}\right) \\ &= \ln\left(\left(1-\frac{4}{n}\right)^{n-1}\right) + O(\frac{n}{2^n}) \end{aligned}$$

Thus

$$T(n) = \left(1-\frac{4}{n}\right)^{n-1} e^{O(n/2^n)} \;\sim\; \frac{1}{e^4}$$

Since the expected size is $2^{n-2}(1-T(n))$, the proof is finished. $\square$

The limiting value is achieved somewhat slowly. For example Maple reveals that $1 - Pr(H(b, S(998, 2^1000/1000) = 1) \approx 0.01816930954$, where the limiting value is $e^{-4} \approx 0.01831563889$. And with $n = 2000$ the approximation is 0.01827898319. An application of trinomial revision to the binomial coefficient ratios in Theorem 3.2 is necessary in order to allow Maple to do the calculation.

Now the question is: How well do these results approximate the actual data? Consider the graph of Figure 2. The black horizontal line is $y = e^{-4} \approx 0.18$. The (green) dots are the scaled data values $1 - I(n, 1)/2^{n-2}$. The upper curve is $1 - Pr(H(b, S(n-1, 2^n/n) = 1)$. The lower curve is from the next subsection. Note that the upper curve is tending to the limiting value (as proven in Theorem 3.1), but that the actual data values seem to be on a trajectory that will blast them through the horizonal line at e^{-4}.

Since the current model does not explain the data, perhaps we need to refine it. In the next two subsections we restrict the random strings to be reverse-closed. Given a binary string b, let b^R represent the reversal of b. A set of binary strings S is *reverse-closed* if $b^R \in S$ whenever $b \in S$.

3.2. **Even length odd density reverse-closed sets.** Let O represent the binary strings of length N with odd density, and let E represent the binary strings of length N with even density. Since N is even, there is no $b \in O$ where $b = b^R$. Therefore, we can partition O into $O^> \cup O^<$ where $O^>$ and $O^<$ are defined as

$$O^> := \{b \in O : b > b^R\} \text{ and } O^< := \{b \in O : b < b^R\}.$$

Let $R = R(N, M)$ be a reverse-closed set of M odd density bitstrings of length N, chosen uniformly at random. Our objective is to calculate the expected size of $\mathcal{N}(R(N, M))$ as a function of M and N. We will write this as $\mathcal{E}[|\mathcal{N}(R(N, M))|]$. Since R is reverse-closed and $b \in O^>$ if and only if $b^R \in O^<$, each string in $R \cap O^>$ is uniquely paired with a string in $R \cap O^<$. Thus M must also be even, and we proceed as if R was constructed by selecting

FIGURE 2. The black horizontal line is $y = e^{-4} \approx 0.18$. The (green) dots are the scaled data values $1 - I(n, 1)/2^{n-2}$. The upper curve is $1 - Pr(H(b, S(n - 1, 2^n/n) = 1)$.

$M/2$ elements from $O^>$. Since $R \subseteq O$, we know that $\mathcal{N}(R) \subseteq E$, and we will find it useful to partition E into $E^= \cup E^{\neq}$ where

$$E^= = \{b \in E : b = b^R\} \text{ and } E^{\neq} = \{b \in E : b \neq b^R\}.$$

This partition of E is useful since

$$|\{c \in O^> : c \in R \implies b \in \mathcal{N}(R)\}| \quad = \quad \begin{cases} N/2 & \text{when } b \in E^= \\ N & \text{when } b \in E^{\neq} \end{cases}$$

For example, when $N = 4$, let us consider the difference between $0000 \in E^=$ and $1010 \in E^{\neq}$. If $0000 \in \mathcal{N}(R)$ then one of $1000, 0100, 0010, 0001$ must be in R, so one of $1000, 0100$ must be in $R \cap O^>$. On the other hand, if $1010 \in \mathcal{N}(R)$ then one of $0010, 1110, 1000, 1011$ must be in R, so one of $0100, 1110, 1000, 1101$ must be in $S \cap O^>$. The difference arises from the fact that two neighbors of $b \in E^=$ can be reverses of each other, but this cannot happen when $b \in E^{\neq}$. Now we are ready to compute $\mathcal{E}[|\mathcal{N}(R)|]$.

First note that $|O| = |E| = 2^{N-1}$, $|O^>| = |O^<| = 2^{N-2}$, $|E^=| = 2^{N/2}$, and $|E^{\neq}| = 2^{N-1} - 2^{N/2}$.

Theorem 3.5. *If N is even then the expected size of the set $\mathcal{N}(R(N, M))$ is*

$$2^{N-1}\left(1 - \frac{\binom{2^{N-2}-N/2}{M/2} + (2^{N/2-1} - 1)\binom{2^{N-2}-N}{M}}{\binom{2^{N-2}}{M/2}}\right)$$

Proof. We compute the probability that a bitstring b is not in $\mathcal{N}(R(N,M))$, assuming that b is even.

$$\begin{aligned}
Pr(b \notin \mathcal{N}(R)) &= Pr(b \notin \mathcal{N}(S)|b \in E^{=})Pr(b \in E^{=}) + \\
& \quad Pr(b \notin \mathcal{N}(S)|b \in E^{\neq})Pr(b \in E^{\neq}) \\
&= \frac{\binom{|O^{>}|-N/2}{M/2}}{\binom{|O^{>}|}{M/2}} \frac{2^{N/2}}{2^{N-1}} + \frac{\binom{|O^{>}|-N}{M/2}}{\binom{|O^{>}|}{M/2}} \frac{2^{N-1}-2^{N/2}}{2^{N-1}} \\
&= \frac{\binom{2^{N-2}-N/2}{M/2}}{\binom{2^{N-2}}{M/2}} \frac{1}{2^{N/2-1}} + \frac{\binom{2^{N-2}-N}{M/2}}{\binom{2^{N-2}}{M/2}} \left(1 - \frac{1}{2^{N/2-1}}\right) && (7) \\
&= \frac{\binom{2^{N-2}-M/2}{N/2}}{\binom{2^{N-2}}{N/2}} \frac{1}{2^{N/2-1}} + \frac{\binom{2^{N-2}-M/2}{N}}{\binom{2^{N-2}}{N}} \left(1 - \frac{1}{2^{N/2-1}}\right). && (8)
\end{aligned}$$

The last equality (8) again follows by trinomial revision and yields a final expression that is better for computation. Since

$$\begin{aligned}
\mathcal{E}[|\mathcal{N}(R)|] &= |E| \cdot Pr(b \in \mathcal{N}(R)) \\
&= |E| \cdot (1 - Pr(b \notin \mathcal{N}(R)))
\end{aligned}$$

the proof is finished. □

Theorem 3.6. *If N is even then*

$$E[|\mathcal{N}(R(n-1, 2^n/n))|] \sim 2^{n-2}(1-e^{-4}).$$

Proof. In Theorem 3.5 the second summand in (7) will clearly dominate asymptotically. Setting $N = n-1$ and $M = 2^n/n$, by Lemma 3.1,

$$\frac{\binom{2^{N-2}-N}{M/2}}{\binom{2^{N-2}}{M/2}} = \frac{\binom{2^{n-3-2}-(n-1)}{2^{n-1}/n}}{\binom{2^{n-3}}{2^{n-1}/n}} \sim \lim_{n\to\infty}\left(1 - \frac{2^{n-1}/n}{2^{n-3}}\right)^{n-1} = \lim_{n\to\infty}\left(1-\frac{4}{n}\right)^{n-1} = e^{-4}.$$

□

A Maple calculation for $n = 1000$ gives 0.01824227864 and for $n = 2000$ we get 0.01827898319, whereas the value of e^{-4} is about 0.01831563889, so again convergence is quite slow.

3.3. **Odd length odd density reverse-closed sets.** The case where N is odd is more complicated because now there are odd density strings b such that $b = b^R$.

Let O represent the binary strings of length N with odd density, and let E represent the binary strings of length N with even density. We can partition O into $O^{=} \cup O^{>} \cup O^{<}$ where $O^{>}$ and $O^{<}$ were defined before and

$$O^{=} = \{b \in O : b = b^R\}.$$

Suppose $R = R(N,M) \subseteq O$ is chosen uniformly at random to be a reverse-closed set of M binary strings of length N. Our objective is to calculate the expected size of $\mathcal{N}(R)$ in terms of M and N. We will write this as $\mathcal{E}[|\mathcal{N}(|R(N,M)|)|]$. Since R is reverse-closed and $b \in O^> \iff b^R \in O^<$, each string in $R \cap O^>$ is uniquely paired with a string in $S \cap O^<$, and the remaining strings in S are in $S \cap O^=$. For this reason, we proceed as if R was constructed by selecting i elements from $O^=$ and then $\frac{M-i}{2}$ elements from $O^>$. Since $S \subseteq O$, we know that $\mathcal{N}(R) \subseteq E$, and we will find it useful to partition E into $E^0 \cup E^1 \cup E^2$ where, for $j = 0, 1, 2$, $E^j = \{b \in E : |\mathcal{N}(\{b\}) \cap O^=| = j\}$.

To illustrate these sets, let us consider one example for each set when $N = 5$. The string $01100 \in E^2$ since $\mathcal{N}(\{b\}) \cap O^= = \{00100, 01110\}$. In general, E^2 contains binary strings in E whose middle bit is one, and who disagree with their reverse in one of the first n positions. In other words, b is in E^2 if $b[n] = 1$, and $b[x] \neq b[N-x]$ has a unique solution for $0 \leq x \leq (N-1)/2$. Then $\mathcal{N}(\{b\}) \cap O^=$ contains the result of changing the xth or $(N-x)$th bit of b. The string $01010 \in E^1$ since $\mathcal{N}(\{b\}) \cap O^= = \{01110\}$. In general, E^1 contains binary strings in E whose middle bit is zero, and who are equal to their reverse. Then $\mathcal{N}(\{b\}) \cap O^=$ contains the result of changing the middle bit of b to one. The string $01001 \in E^2$ since $\mathcal{N}(\{b\}) \cap O^= = \emptyset$. In general, E^0 contains the binary strings in E that are not in E^2 or E^1.

This partition of E is useful since

$$|\{c \in O^= : c \in R \implies b \in \mathcal{N}(R)\}| = \begin{cases} 0 & \text{when } b \in E^0 \\ 1 & \text{when } b \in E^1 \\ 2 & \text{when } b \in E^2 \end{cases}$$

and

$$|\{c \in O^> : c \in R \implies b \in \mathcal{N}(R)\}| = \begin{cases} N & \text{when } b \in E^0 \\ (N-1)/2 & \text{when } b \in E^1 \\ N-2 & \text{when } b \in E^2 \end{cases}$$

For example, when $N = 5$, let us consider the difference between $01100 \in E^2$, $01010 \in E^1$, and $01001 \in E^0$. If $01100 \in \mathcal{N}(R)$ then one of $11100, 00100, 01000, 01110, 01101$ must be in S, so one of $00100, 01110$ must be in $R \cap O^=$, or one of $11100, 01000, 10110$ must be in $S \cap O^>$. If $01010 \in \mathcal{N}(R)$ then one of $11010, 00010, 01110, 01000, 01011$ must be in R, so 01110 must be in $R \cap O^=$, or one of $11010, 01000$ must be in $S \cap O^>$. Finally, if $01001 \in \mathcal{N}(S)$ then one of $11001, 00001, 01101, 01011, 01000$ must be in R, so one of $11001, 10000, 10110, 11010, 01000$ must be in $R \cap O^>$. The main thing to notice is that two neighbors of $b \in E^1$ can be reverses of each other, but this cannot happen when $b \in E^0 \cup E^2$. Now we are ready to compute $\mathcal{E}[|\mathcal{N}(R)|]$.

Note that $|O| = 2^{N-1}$ where $|O^=| = 2^{(N-1)/2}$, and $|O^>| = |O^<| = 2^{N-2} - 2^{(N-3)/2}$. Similarly, $|E| = 2^{N-1}$, $|E^2| = (N-1)2^{(N-3)/2}$, $|E^1| = 2^{(N-1)/2}$, and $|E^0| = 2^{N-1} - (N+1)2^{(N-3)/2}$.

As before we can determine the expected size of the neighborhood by first deriving a certain probability, since

$$\begin{aligned} \mathcal{E}[|\mathcal{N}(|R(N,M)|)|] &= |E| Pr(b \in \mathcal{N}(S) | b \in E) \\ &= |E|(1 - Pr(b \notin \mathcal{N}(S) | b \in E)). \end{aligned}$$

In each of the sums below, the summation is over all $i = 0, 1, \ldots, M$ such that $(M-i)/2$ is an integer (i.e., such that M and i have the same parity).

$$\begin{aligned} Pr(b \notin \mathcal{N}(S)|b \in E) &= Pr(b \notin \mathcal{N}(R)|b \in E^2)Pr(b \in E^2|b \in E) + \\ & \quad Pr(b \notin \mathcal{N}(R)|b \in E^1)Pr(b \in E^1|b \in E) + \\ & \quad Pr(b \notin \mathcal{N}(R)|b \in E^0)Pr(b \in E^0|b \in E) \\ &= \left(\sum \frac{\binom{|O^=|-2}{i}}{\binom{|O^=|}{i}} \frac{\binom{|O^>|-(N-2)}{(M-i)/2}}{\binom{|O^>|}{(M-i)/2}} \right) \frac{N-1}{2^{(N+1)/2}} + \\ & \quad \left(\sum \frac{\binom{|O^=|-1}{i}}{\binom{|O^=|}{i}} \frac{\binom{|O^>|-(N-1)/2}{(M-i)/2}}{\binom{|O^>|}{(M-i)/2}} \right) \frac{1}{2^{(N-1)/2}} + \\ & \quad \left(\sum \frac{\binom{|O^>|-N}{(M-i)/2}}{\binom{|O^>|}{(M-i)/2}} \right) \left(1 - \frac{N+1}{2^{(N+1)/2}} \right) \end{aligned}$$

We will make use of the following nice identity. The first equality is contained in Gould's [4] classic tables of binomial coefficient identities (identity (4.1)). The second can be easily verified.

$$\sum_{k=j}^{n} \frac{\binom{z}{k}}{\binom{x}{k}} = \frac{x+1}{x-z+1} \left\{ \frac{\binom{z}{j}}{\binom{x+1}{j}} - \frac{\binom{z}{n+1}}{\binom{x+1}{n+1}} \right\} = \frac{x-n}{z-x-1} \frac{\binom{z}{n+1}}{\binom{x}{n+1}} - \frac{x-j+1}{z-x-1} \frac{\binom{z}{j}}{\binom{x}{j}} \tag{9}$$

These identities and others can be used to eliminate the sums above, and we can then determine the asymptotics as before. These details will have to await the full paper.

References

[1] A. Bérczes and L. Hajdu, *Computational Experiences on the Distances of Polynomials to Irreducible Polynomials*, Mathematics of Computation, 66 (1997) 391–398.

[2] K. Cattell, F. Ruskey, J. Sawada, C.R. Miers, and M. Serra, *Fast Algorithms to Generate Necklaces, Unlabelled Necklaces and Irreducible Polynomials over GF(2)*, J. Algorithms, 37 (2000) 267–282.

[3] S. D. Cohen, *Uniform distribution of polynomials over finite fields*, Journal of the London Mathematical Society, 6 (1972) 93–102.

[4] H. W. Gould, *Combinatorial Identities*, Morgantown Printing and Binding, Morgantown, VA., 1972.

[5] D. R. Hayes, *The distribution of irreducibles in* $GF[q,x]$, Transactions of the American Mathematical Society, 117 (1965) 101–127.

[6] Dieter Jungnickel, *Finite Fields: Structure and Arithmetics*, BI-Wissenschaftsverlag, Mannbeim, 1993.

[7] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press, 1994.

[8] D.E. Knuth, R.L. Graham, and O. Patashnik, *Concrete Mathematics*, Second edition, Addison-Wesley, 1989.

[9] S. Uchiyama, *Sur les polynomes irréductibles dans un corps fini. II.*, Proc. Japan Acad., 31 (1955) 267–269.

Dept. of Computer Science, University of Victoria, CANADA

Dept. of Computer Science, University of Victoria, CANADA
URL: `http://www.cs.uvic.ca/~ruskey`

Dept. of Computer Science, University of Victoria, CANADA