Binary Strings and Graphs

Dr. Gregory Hartman, Matthew Green

May 21, 2004

1 Introduction

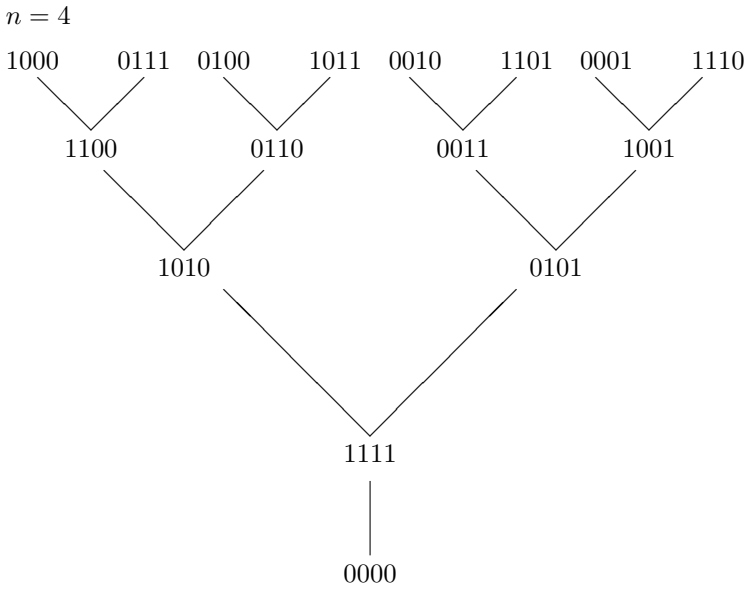
Binary strings of length n can be added and permuted. Of special interest is the permutation that cyclicly shifts a binary string to the right. For example, when $n = 5$, then cyclicly shifting 10110 to the right yields 01011. Obviously if we cyclicly shift a string of length n to the right n times to get back what we started with. Addition of the strings is done component-wise modulo 2. For instance, when $n = 7$, then $1011000 + 1100101 = 0111101$. We spent the semester studying the operation that cyclicly shifts a string to the right once, and then adds the result back to the original. Here are some examples for when $n = 4$: $1010 \to 1111$, $1000 \to 1100$ and $0111 \to 1100$.

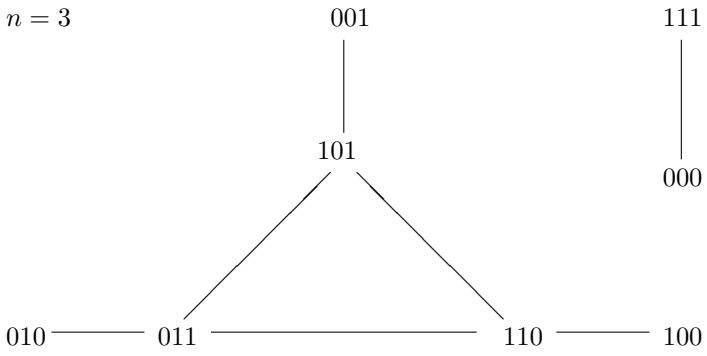
Definition: Let B_n be the set of binary strings of length n. Define $r : B_n \to B_n$ to be the operation that cyclicly shifts each string s in B_n to the right once. Now let $1+r : B_n \to B_n$ be defined by the equation $(1+r)(s) = s+r(s)$ for all s in B_n.

It is useful to observe the property that $r(s + t) = r(s) + r(t)$ for all s and t in B_n. Then by definition we have $(1 + r)(s + t) = (s + t) + r(s + t) = (s + r(s)) + (t + r(t)) = (1 + r)(s) + (1 + r)(t)$ for all s and t in B_n.

Starting with some element s_0 in B_n we apply the operation $1 + r$ over and over, forming a set $\{s_0, s_1, s_2, \ldots, s_m\}$, where $s_{i+1} = (1 + r)(s_i)$. We call this set the orbit of s_0 under the operation $1 + r$. Since B_n is finite, the orbit of any binary string is also finite. Thus for any s_0 in B_n, there is a positive integer m such that $s_{m+1} = s_k$ for some positive integer k, with $0 \leq k \leq m$.

We made graphs of the orbits of the elements of B_n for several different choices of n. Included here are the graphs of $n = 3$ and $n = 4$:





Upon inspection of the graphs some questions naturally arise. The graph of $n = 4$ is clearly a tree and has no cycles. In this case, repeatedly applying $1 + r$ to any string eventually gives you the zero string. Is this the case whenever $n = 2^k$ for $k \geq 1$? When $n = 3$ the orbit graph has two components, one of which has a cycle of length 3. How can we predict the number cycles and the length of those cycles in the orbit graph for a given string length n?

2 Preliminaries

If you study the example graphs carefully you may find that only those strings that have an odd number of $1's$ populate the outer regions of the graphs. For

brevity, we give the following definition.

Definition: Let $s \equiv a_1 a_2 \dots a_n$ be an element of B_n. The weight of s, denoted $w(s)$, is defined as $w(s) = \sum_{i=1}^{n} a_i$.

For example, the string 10011 has weight 3.

Thinking of binary strings as nodes in the graph (from here on out we use the term 'string' and 'node' interchangeably), the strings of odd weight are those nodes that do not have any parent nodes. This means that no string is mapped to a string of odd weight under the operation $1 + r$.

Theorem 1.1. If s be an element of B_n then $(1 + r)(s)$ has even weight.

Proof. Let $t = (1 + r)(s) = s + r(s) \equiv t_1 t_2 \dots t_n$, $s \equiv a_1 a_2 \dots a_n$ and $r(s) \equiv b_1 b_2 \dots b_n$. Clearly if $w(s) = m$, then $w(r(s)) = m$. At each index i that $a_i = b_i$ we have $t_i = 0$. In the case that $a_i \neq b_i$ for $i = 1, 2, \dots, n$, the weight of t is equal to $2m$ (the total number of 1's in s and r(s)). Thus we can calculate the weight of t by subtracting 2 from $2m$ each time $a_i = b_i = 1$. So $w(t) = 2m - 2k = 2(m-k)$, where k is the number of indices i at which $a_i = b_i = 1$.

Another observation is that each node of even weight has two parent nodes and the parent nodes add to the string with all components equal to 1.

Theorem 1.2. The inverse image under the operation $1 + r$ of any non-zero string s in B_n that has even weight is a two element set. Furthermore, two distinct non-zero strings s and t in B_n have the property that $(1+r)(s) = (1+r)(t)$ if and only if $s+t = 1$, where $\imath$ denotes the string with all components equal to 1.

Proof. Let s and t be two distinct non-zero strings in B_n such that $(1+r)(s) = (1 + r)(t)$. Rearranging we obtain $r(s + t) = (s + t)$. The only strings that are fixed by $1 + r$ are the string of all 1's, denoted by $\imath$, and the string of all 0's, denoted by o. So either $s + t = o$ or $s + t = \imath$. But we assumed that s and t are distinct, so $s + t = \imath$. Conversely, assume $s + t = \imath$. Applying $1 + r$ to both sides of the equation yields $(1 + r)(s) + (1 + r)(t) = (1 + r)(\imath) = \imath + \imath = o$. Thus $(1+r)(s) = (1+r)(t)$. Now suppose we have a string $a \equiv a_1 a_2 \dots a_n$ with even weight in B_n. Observe that $w(a) \bmod 2 = \sum_{i=1}^{n} a_i \bmod 2 = 0$. Doing all arithmetic modulo 2, it follows that $a_n + \sum_{i=1}^{n-1} a_i = 0$, so $a_n = \sum_{i=1}^{n-1} a_i$. With this observation we can find a string $s \equiv s_1 s_2 \dots s_n$ such that $(1 + r)(s) = a$ in the following manner: Assume, without loss of generality, that $s_1 = 1$. We know that the components of s must satisfy the sequence of equations $s_1 + s_n = a_1$, $s_2 + s_1 = a_2$, $s_3 + s_2 = a_3$, $\dots$, $s_n + s_{n-1} = a_n$. Since we have taken $s_1 = 1$, we can define $s_k = a_k + a_{k-1} + \cdots + a_2 + 1$ for $k = 2, 3, \dots, n$. This definition must satisfy $s_n + s_{n-1} = a_n$. But this is equivalent to $a_n = (a_1 + 1) + (a_{n-1} + \dots + a_2 + 1) = \sum_{i=1}^{n-1} a_i$, which we already

know. The string $\imath + s$ is the second parent. There are no other parents because if $t \neq s$ and $t \neq s + \imath$, then $t + s \neq \imath$ and $t + s + \imath \neq \imath$.

We still have not addressed the question of when cycles form in the orbit graph and how long they are. We could continue to analyze the problem using only strings of zeros and ones and the addition and shifting operations. But as you may have noticed, the proofs so far have been cumbersome, especially considering the simple results that they yield. So we looked for another way to represent the binary strings, which would allow for a more elegant and powerful analysis. We present this new representation before returning to the question of the cycles.

3 Polynomials and Ideals

The representation of binary strings of length n as polynomials of degree less than n with coefficients in the finite field F_2 is an easy and powerful representation to work with. For example, if $n = 5$ then we can write the string 11111 as $1 + x + x^2 + x^3 + x^4$ and 01101 turns into $x + x^2 + x^4$. The operation of cyclicly shifting a string to the right can be represented as polynomial multiplication by x. For instance, shifting 10110 to 01011 is equivalent to multiplying $1 + x^2 + x^3$ by x, yielding $x + x^3 + x^4$. Component-wise addition of strings is easily represented by regular polynomial addition, keeping in mind that coefficients are in F_2 so arithmetic is done modulo 2. Also since cyclicly shifting a string of length n to the right n times gives you back what you started with, we have $x^n = 1$, which means that $1+x^n = 0$. This leads to the following definition:

Definition: Let n be a positive integer. Define $R_n = F_2[x]/\langle 1 + x^n \rangle$. As a set, $R_n = \{a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} : a_i \in F_2\}$.

The additive group of this ring is isomorphic to our old set of binary strings of length n, which we called B_n. Since B_n is an abelian group, it can be thought of as a $\mathbb{Z}$-module. The operation $1 + r$ that acted on B_n is just one element of the endomorphism ring $\mathrm{End}_{\mathbb{Z}}(B_n)$. This element corresponds to the element $1+x$ in R_n; in fact, since the element $x \in R_n$ generates R_n, it is easy to see that R_n is isomorphic as rings to the subring of $\mathrm{End}_{\mathbb{Z}}(B_n)$ generated by the element r. Thus much of our study of B_n under the operation of $1 + r$ can be done by studying R_n as a R_n-module.

It follows from the definition of R_n and the fact that $F_2[x]$ is a principal ideal domain that R_n is a principal ring. Thus every ideal I of R_n is generated by polynomial of minimal degree in I. If $g(x)$ generates I we write $I = \langle g(x) \rangle$.

An immediate application of this new perspective is the following theorem:

Theorem 2.1. The orbit graph associated with R_{2^k} for positive integers $k \geq 0$ is a maximal binary tree.

Proof. Since the field F_2 has characteristic 2, if $f(x)$ is in R_{2^k}, then $f(x)^{2^k} = f(x^{2^k})$. So for any $f(x)$ in R_{2^k} we have $(1+x)^{2^k}(f(x)) = (1+x^{2^k})(f(x)) = f(x) + f(x) = 0$. In the case that $k = 0$ we have a trivial tree of one node. So assume that $k \geq 1$. Starting at the zero string, we find it has exactly two parent nodes: the string of all ones and itself. Moving up to the string of all ones, we also find that it has exactly two parents. Moving up again, we find that each parent has exactly two parents. Since every node is path-connected to the zero string node, we can reach every node of the graph by starting at the zero string and moving up in this fashion. We can also keep count of how many nodes we have reached as we move up from the zero string. This is easy to do: moving up from the zero string we find $1 = 2^0$ more node. Moving up again we find $2 = 2^1$ more nodes. Moving up again we find $4 = 2^2$ more nodes. In general, if we move up m times from the zero node we will reach $\sum_{i=0}^{m-1} 2^i = 2^m - 1$ nodes. So if we move up k times from the zero node we reach $2^k - 1$ nodes, and adding in the zero node to the count gives us all 2^k nodes. In the process we have mapped out a tree.

The condition for a polynomial $f(x)$ in R_n to be a member of a cycle is that $(1+x)^k f(x) = f(x)$ for some $k \geq 1$. Also notice that for $f(x)$ in R_n to be a member of a cycle, it follows from Theorem 1.1 that the string represented by $f(x)$ must have even weight. This is equivalent to the condition that $1+x|f(x)$. This leads us to think about the ideal structure of R_n, and in particular the ideal $\langle 1+x \rangle$.

We made brute force computations of the orbit graphs for n less than 120 using a computer and found some interesting results. We found no regular pattern that gave us the number of cycles and the cycle lengths. For instance, when $n = 7$ we obtain 9 cycles of order 7; when $n = 21$ we get 1 cycle of length 3, 9 cycles of length 7, 9 cycles of length 21, and 16640 cycles of length 63. This initially led to a guess that maximal cycle length would be given by $2^{\phi(n)} - 1$, where $\phi(n)$ is the multiplicative order of 2 modulo n. But this turns out not to be the case.

Further pursuing an analysis of the ideals of R_n we find a nice correspondence between ideals and divisors of $1 + x^n$.

Theorem 2.2. An ideal I of R_n is generated by a polynomial $g(x)$ if and only if $g(x)$ divides $1 + x^n$.

Proof. Let I be an ideal of R_n and suppose that $g(x)$ generates I. We can divide $1 + x^n$ by $g(x)$ in $F_2[x]$ using the division algorithm, yielding $1 + x^n = q(x)g(x) + r(x)$, where $deg(r(x)) < deg(g(x))$. Reducing modulo $1 + x^n$ we obtain $0 = q(x)g(x) + r(x)$ in R_n so that $r(x) = q(x)g(x)$, which implies that $r(x)$ is a member of I. But $g(x)$ generates I, which means $g(x)$ is a monic polynomial of minimal degree in I, so $r(x) = 0$ and $g(x)|(1 + x^n)$.

Conversely, assume $f(x)|(1+x^n)$, $f(x) \neq 1+x^n$. Then there is a polynomial

$h(x)$ in $F_2[x]$ so that $1 + x^n = f(x)h(x)$. Let $I = \langle f(x)\rangle$ in R_n and suppose that $g(x)$ generates I. Since $g(x)$ has minimal degree in I, we have $deg(g(x)) \leq deg(f(x))$. As $g(x)$ is a member of $I = \langle f(x)\rangle$, there is an element $k(x)$ in R_n such that $g(x) = k(x)f(x)$. Thus $g(x)h(x) = k(x)f(x)h(x) = k(x)(1 + x^n) = 0$ in R_n. This means that $deg(g(x)) \geq deg(f(x))$, which together with the inequality above implies that $deg(f(x)) = deg(g(x))$. Now we have two polynomials, $f(x)$ and $g(x)$ of minimal degree d in I. Both are monic so the polynomial $f(x) - g(x)$ is in I and has degree less than d. Therefore $f(x) - g(x) = 0$, showing that $f(x) = g(x)$.

To describe all the ideals of R_n we can factor $1 + x^n$ into a product of irreducible factors and combinations of these factors correspond to ideals of R_n. For example, $1+x^7=(1+x)(1+x+x^3)(1+x^2+x^3)$, so the ideals of R_7 are precisely $\langle 1+x\rangle$, $\langle 1+x+x^3\rangle$, $\langle 1+x^2+x^3\rangle$, $\langle (1+x)(1+x+x^3)\rangle$, $\langle (1+x)(1+x^2+x^3)\rangle$, $\langle (1+x+x^3)(1+x^2+x^3)\rangle$, $\langle 0\rangle$ and R_n. If we restrict n to be odd, something lovely happens. Among the ideals of R_n consider the minimal ideals, that is, those ideals which contain no other ideals besides the trivial ideal. Minimal ideals can be easily described in the following way:

Theorem 2.3. Let n be odd and $1 + x^n = f_1(x)f_2(x)\cdots f_m(x)$ be a factorization of $1 + x^n$ into a product of m irreducible factors. The minimal ideals M_i of R_n are given by $M_i = \langle (1 + x^n)/f_i(x)\rangle$ for $i = 1, 2, \ldots, m$.

Proof. Let $1 + x^n = f_1(x)f_2(x)\cdots f_m(x)$ be a factorization of $1 + x^n$ into a product of m irreducible factors. Set $g_i(x) = (1 + x^n)/f_i(x)$ for $i = 1, 2, \ldots, m$ and define $M_i = \langle g(x)\rangle$ for $i = 1, 2, \ldots, m$. The ideals of R_n correspond with divisors of $1 + x^n$, so to determine whether or not there is a non-trivial ideal contained in M_i, for each $i = 1, 2, \ldots, m$, we need to check if there is a divisor $f(x)$ of $1 + x^n$ such that $g_i(x)|f(x)$. Clearly the only polynomial $f(x)$ satisfying this condition is $1 + x^n$. Therefore only the trivial ideal $\langle 1 + x^n\rangle = \langle 0\rangle$ is contained in each M_i.

Now it is possible to express R_n as a direct sum of its minimal ideals. Not only that, but if n is odd, then each minimal ideal is actually a field in R_n. To show this we begin with a theorem on idempotent elements in the minimal ideals.

Theorem 2.4. Let n be an odd positive integer and let M be a minimal ideal of R_n. Then there is a idempotent element $\theta(x)$ in M such that $\theta(x)$ is an identity element in M and $M = \langle \theta(x)\rangle$.

Proof. Let n be an odd positive integer. Set $g(x) = (1 + x^n)/f(x)$, where $f(x)$ is a proper irreducible divisor of $1 + x^n$, and suppose that $M = \langle (1 + x^n)/f(x)\rangle$ is a minimal ideal of R_n. Since $\gcd(f(x), g(x)) = 1$, we can find elements $a(x)$ and $b(x)$ in $F_2[x]$ such that $a(x)g(x) + b(x)f(x) = 1$. Define $\theta(x) = a(x)g(x) \bmod 1 + x^n$ and let $k(x)$ be an element of M. Note first that $k(x)f(x) = 0$ in R_n. Then $k(x) = k(x) \cdot 1 = k(x)[a(x)g(x) + b(x)f(x)] =$

$\theta(x)k(x)+b(x)f(x)k(x) = \theta(x)k(x)$ (where our reference here to $a(x), b(x), f(x)$ and $g(x)$ really refer to their reductions modulo $1 + x^n$). This shows that $\theta(x)$ is an identity element of M. A similar argument shows that $\theta(x)\theta(x) = \theta(x)$ so that $\theta(x)$ is an idempotent element of R_n.

The following theorems are essential to arrive at our main result:

Theorem 2.5. Suppose n is an odd positive integer and let $\{M_1, M_2, \ldots, M_m\}$ be a collection of all minimal ideals of R_n. Let $\{\theta_1(x), \theta_2(x), \ldots, \theta_m(x)\}$ be the set of generating idempotents for the minimal ideals of R_n, where $M_i = \langle \theta_i(x) \rangle$ for $i = 1, 2, \ldots, m$. Then $\theta_1(x) + \theta_2(x) + \cdots + \theta_m(x) = \sum_{i=1}^{m} \theta_i(x) = 1$ and $\theta_i\theta_j = 0$ when $i \neq j$.

Theorem 2.6. Let n be an odd positive integer and let M be a minimal ideal of R_n and suppose $g(x)$ of degree d generates M. Then M is a field isomorphic to F_{2^k}, where $k = n - d$.

Theorem 2.7. Let n be a positive odd integer and suppose $\{M_1, M_2, \ldots, M_m\}$ is a collection of all the minimal ideals of R_n. Then $R_n = M_1 \bigoplus M_2 \bigoplus \cdots \bigoplus M_m$.

Proof. Set equality follows directly from Theorem 2.5, since if $f(x)$ is in R_n then $f(x) = f(x) \cdot 1 = f(x)\theta_1(x) + f(x)\theta_2(x) + \cdots + f(x)\theta_m(x)$, where $f(x)\theta_i(x)$ is reduced modulo $1 + x^n$ for each $i = 1, 2, \ldots, m$. If $f(x)$ and $g(x)$ are elements of R_n, then $\sum_{i=1}^{m}(f(x) + g(x))\theta_i(x) = \sum_{i=1}^{m} f(x)\theta_i(x) + \sum_{i=1}^{m} g(x)\theta_i(x)$ and $\sum_{i=1}^{m} f(x)g(x)\theta_i(x) = f(x)g(x)\sum_{i=1}^{m}(\theta_i(x))^2 = f(x)g(x)[\sum_{i=1}^{m} \theta_i(x)]^2 = [\sum_{i=1}^{m} f(x)\theta_i(x)] \cdot [\sum_{i=1}^{m} g(x)\theta_i(x)]$. This shows ring equivalence.

So for odd positive integers n we can decompose R_n into a direct sum of fields. This fact is highly suggestive that components of the orbit graph somehow correspond with the component fields of R_n.

Definition: Let n be odd and let $R_n = M_1 \bigoplus M_2 \bigoplus \cdots \bigoplus M_m$ with each M_i a minimal ideal in R_n, for $i = 1, 2, \ldots, m$. Let $f(x)$ be an element in R_n. Then the projection of $f(x)$ in the component M_i is given by $f(x)\theta_i(x)$, where $\theta_i(x)$ is the generating idempotent in M_i.

If $R_n = M_1 \bigoplus M_2 \bigoplus \cdots \bigoplus M_m$ is a decomposition of R_n into component fields then we can look at the multiplicative order of the projection $(1+x)\theta_i(x)$ within each M_i to tell us when exactly $((1+x)\theta(x))^k f(x) = (1+x)^k f(x) = f(x)$ for non-zero $f(x)$ in M_i. A nice property of finite fields is that the non-zero elements of a finite field form a multiplicative group. So we can study the subgroup generated by $(1 + x)\theta_i(x)$ within $M_i - \{0\}$.

Definition: Let n be an odd positive a integer and suppose $f(x)$ is in R_n and is of even weight. Define the cycle order of $f(x)$ to be

Theorem 2.8. Let n be an odd positive integer. Suppose $R_n = M_1 \bigoplus M_2 \bigoplus \cdots \bigoplus M_m$ is a decomposition of R_n into component fields. For each index i let $\rho_i(x) = (1+x)\theta_i(x)$ denote the projection of $1+x$ in M_i. Form the power set $P = P(M_1, M_2, \ldots, M_m)$ of the component fields. Then for each $A = \{M_{\alpha_1}, M_{\alpha_2}, \ldots, M_{\alpha_k}\}$ in P, the cycle order of each element in $\bigoplus_{i=1}^{k} M_{\alpha_i}$ is given by $l_A = lcm(|\rho_{\alpha_1}|, |\rho_{\alpha_2}|, \ldots, |\rho_{\alpha_k}|)$.

Proof. We can partition each M_i^* into left (or right) cosets of the subgroup $\langle \rho_i \rangle$. Each distinct coset $a\langle \rho_i \rangle$ corresponds to a cycle, since each coset is closed under multiplication by ρ_i. The order of each coset is $|\langle \rho_i \rangle|$, and this gives the length of the cycle. The number of cosets $|M_i^*|/|\langle \rho_i \rangle|$ is the number of cycles associated with the cosets $a\langle \rho_i \rangle$ in M_i^*. Counting and measuring the cycles corresponding to each M_i^* individually, is equivalent to counting and measuring the cycles corresponding to the subgroup $0 \bigoplus 0 \bigoplus \ldots \bigoplus M_i^* \bigoplus \ldots \bigoplus 0 \cong M_i^*$ of the multiplicative group $M_1^* \bigoplus M_2^* \bigoplus \ldots \bigoplus M_m^*$. But we must also count and measure the cycles corresponding to the cases where we have more than one non-zero component. So for each element $A = \{M_{\alpha_1}, M_{\alpha_2}, \ldots, M_{\alpha_k}\}$ in the power set $P = P(M_1, M_2, \ldots, M_m)$, we count and measure the cycles corresponding to $\bigoplus_{i=1}^{k} M_{\alpha_i}^*$. The cycle order l_A of each element in $\bigoplus_{i=1}^{k} M_{\alpha_i}^*$ is the smallest number divisible by $|\rho_{\alpha_i}|$ for $i = 1, 2, \ldots, k$; thus $c_A = lcm(|\rho_{\alpha_1}|, |\rho_{\alpha_2}|, \ldots, |\rho_{\alpha_k}|)$. The number of cycles of length l_A corresponding to $\bigoplus_{i=1}^{k} M_{\alpha_i}^*$ is $c_A = |\bigoplus_{i=1}^{k} M_{\alpha_i}^*|/l_A$.

Here are some examples:

Let $n = 7$. Then $1 + x^7 = (1+x)(1+x+x^3)(1+x^2+x^3)$ and $R_7 = M_1 \bigoplus M_2 \bigoplus M_3 = \langle (1+x)(1+x+x^3) \rangle \bigoplus \langle (1+x)(1+x^2+x^3) \rangle \bigoplus \langle (1+x+x^3)(1+x^2+x^3) \rangle$. Using theorem 2.6 we obtain $R_n \cong F_8 \bigoplus F_8 \bigoplus F_2$. Since the order of multiplicative group of non-zero elements in each component field is prime, it is easy to calculate the multiplicative order of the projection of $1+x$ in each field. Indeed, we have $|\rho_1| = |\rho_2| = 7$ and $|\rho_3| = 1$. The power set P is the set $\{0, \{M_1\}, \{M_2\}, \{M_1, M_2\}, \{M_1, M_3\}, \{M_2, M_3\}, \{M_1, M_2, M_3\}\}$ Thus we have two cycles of length 7 corresponding to M_1 and M_2 individually. Since $|M_3^*| = 1$, we have $M_1^* \cong M_1^* \bigoplus M_3^*$ and $M_2^* \cong M_2^* \bigoplus M_3^*$, so we obtain no new cycles by considering $M_1^* \bigoplus M_3^*$ and $M_2^* \bigoplus M_3^*$. There are 49 elements in $M_1^* \bigoplus M_2^*$ each with cycle order 7, so 7 cycles of order 7 correspond to $M_1^* \bigoplus M_2^*$. Again, we need not consider $M_1^* \bigoplus M_2^* \bigoplus M_3^*$ since it is isomorphic with $M_1^* \bigoplus M_2^*$. So it total there are 9 cycles of order seven along with the zero element. This accounts for all of the even weighted elements since $2^6 = 64 = 9 \cdot 7 + 1$.

Let $n = 21$. Then $1+x^{21} = (1+x)(1+x+x^2)(1+x+x^3)(1+x^2+x^3)(1+x+x^2+x^4+x^6)(1+x^2+x^4+x^5+x^6)$ and $R_n = M_1 \bigoplus M_2 \bigoplus M_3 \bigoplus M_4 \bigoplus M_5 \bigoplus M_6 = \langle (1+x^{21})/(1+x^2+x^4+x^5+x^6) \rangle \bigoplus \langle (1+x^{21})/(1+x+x^2+x^4+x^6) \rangle \bigoplus \langle (1+$

$x^{21})/(1+x^2+x^3)\rangle \bigoplus \langle (1+x^{21})/(1+x+x^3)\rangle \bigoplus \langle (1+x^{21})/(1+x+x^2)\rangle \bigoplus \langle (1+x^{21})/(1+x)\rangle$. By theorem 2.6 we have $R_{21} \cong F_2 \bigoplus F_4 \bigoplus F_8 \bigoplus F_8 \bigoplus F_{64} \bigoplus F_{64}$. In this case, two of the component fields have non-zero element multiplicative groups of composite order 63, but we luck out and find that the projection of $1+x$ in each of these component fields is a primitive element. Using the method given in theorem 2.8, we obtain 1 cycle of order 3 corresponding to M_2^*, 9 cycles of order 7 corresponding to M_3^*, M_4^* and $M_3^* \bigoplus M_4^*$, 9 cycles of order 21 corresponding to $M_2^* \bigoplus M_3^*$, $M_2^* \bigoplus M_4^*$ and $M_2^* \bigoplus M_3^* \bigoplus M_4^*$, 16640 cycles of order 63 corresponding to a variety of other combinations of the M_i (we leave it to the reader to find these combinations explicitly), and the zero string. This indeed accounts for all the even weighted elements since $2^{20} = 1 + 3 + 9 \cdot 7 + 9 \cdot 21 + 16640 \cdot 63$.

Theorem 2.8 gives us a formal way to find the number of cycles of a specific length in the orbit graph of R_n when n is odd. However we are still faced with the difficulty of finding the multiplicative order of the projection of $1+x$ in each of the component fields. Sometimes this is easy, as in the case where the multiplicative group of non-zero elements in the component field has prime order, but in general this requires some non-trivial computation.

We have also neglected the case when n is even. Under this condition, the minimal ideals of R_n are not necessarily fields and we do not have the nice decomposition of R_n into a direct sum of fields. Future goals of this project will be to secure a theory for the case when n is even, and also to generalize to different number bases other than base 2 (this would mean working with polynomials with coefficients in F_n for $n \geq 2$).

4 Reference:

Roman, Steven. *Coding and Information Theory.* Springer-Verlag Graduate Texts in Mathematics, 1992.