Уважаемые студенты групп ИКТУ – 87,88

В конце последней лекции, 1.03.2021, мне были заданы несколько вопросов, на которые я не успел дать подробные ответы в связи с окончанием лекции, и мы договорились, что я постараюсь прислать ответы через личный кабинет в электронном виде.

На вопрос Смирновой Алёны об умножении элементов поля Галуа с помощью характеристической матрицы я ей ответил, указав по её просьбе учебное пособие, где это подробно рассмотрено. Поэтому, кого также интересует этот вопрос, обратитесь к Алёне. Она, надеюсь, не откажет в консультации.

Вопросы, заданные мне в конце лекции Рябинским Егором и Баталиным Никитой практически на одну и ту же тему, связанную со свойствами полей Галуа. Эти вопросы были поставлены следующим образом:

«Для заданного полинома показать, что он не является неприводимым. Для этого попытаться строить соответствующее поле Галуа» (*Рябинский Егор*). И вопрос от *Никиты Баталина*: «Поле, образованное полиномом четвертой степени, становится циклическим с 7-ого элемента, а не с 16-ого, как должно быть. Является ли это признаком того, что полином является неприводимым?».

Сразу, отвечая на вопрос Никиты, говорю – НЕТ, не является. И это станет понятным после подробного ответа с примерами на выше поставленные вопросы и Егора, и Никиты. Эти вопросы надо было рассмотреть подробно не лекции, но времени категорически не хватает и поэтому рассмотрим это дополнительно через личный кабинет. Сразу хочу отметить, если бы студенты хорошо разобрались с теорией полей Галуа, то, возможно, такие вопросы и не возникли бы. Тем не менее, вопросы поставлены и я постараюсь на них дать подробный ответ учитывая, что это нам понадобится в дальнейшем при изучении циклических кодов.

Итак, перейдем к рассмотрению примеров.

Пусть нам задан полином m-ой степени P(x) и нам необходимо определить – является ли он неприводимым, пытаясь строить по нему поле Галуа GF(2m). Для решения этого необходимо взять элемент ε, считая его корнем полинома P(x), т.е. P(ε)=0(modP(x)), и начать его возводить в последовательные степени - εi, *i*=1,2,3,…с приведением ε*i* по modP(x). Зафиксировать ближайшее значение *i*>0, при котором Если то полином P(x) является примитивным и, следовательно, неприводимым. Если же то полином не будет примитивным, но он может быть как неприводимым, так и приводимым. В этом случае необходимо определить, является ли число делителем числа Если *i –* делитель порядка циклической мультипликативной группы элементов поля GF(2m), то он будет неприводимым и будет входить в состав сомножителей разложения двучлена а сам этот двучлен, в соответствии со свойством 1.7, будет делителем двучлена . При этом, если степень полинома P(x) является делителем числа m, то, в соответствии со свойством 1.8, такой полином будет неприводимым. В противном случае полином P(x) будет приводимым, т.е. раскладываться на сомножители с коэффициентами 0 и 1 в простом поле GF(2),.

Рассмотрим этот вопрос на конкретном примере двоичных (p=2) полиномов со степенью m=4.

Предположим у нас не оказалось таблиц с неприводимыми полиномами и мы должны найти неприводимый примитивный полином 4-ой степени и построить поле GF(24). Учтем при этом, что любой неприводимый полином не должен делиться на *x* и (1*+x*). Известно, что полином 4-ой степени не делится на *x,* если он будет примарным, т.е. иметь вид Такой полином также не будет делиться на (1*+x*), если он будет иметь нечетное число ненулевых слагаемых. Поэтому для построения поля GF(24) будем выбирать полином 4-ой степени из множества:

P1(x)= x4 +x +1; P2(x)= x4 +x2 +1; P3(x)= x4 +x3 +1; P4(x)= x4 + x3 + x2 +x +1.

Будем выбирать требуемый полином путём подбора.

Пусть выберем полином P1(x)= x4 +x +1. Примем ε за корень полинома и будем строить поле GF(24), возводя ε в последовательные степени *i*>0 до появления равенства :

|  |  |  |
| --- | --- | --- |
| ε | ε6=ε2+ε3 | ε11=ε+ε2+ε3 |
| ε2 | ε7= ε3+ε4=1+ε+ε3 | ε12=1+ε+ε2+ε3 |
| ε3 | ε8=ε+ε2+ε4=1+ε2 | ε13=1+ε2+ε3 |
| ε4=1+ε | ε9=ε+ε3 | ε14=1+ε3 |
| ε5=ε+ε2 | ε10=ε+ε4=1+ε+ε2 | ε15 |

Так как степень при которой , то полином P1(x) является примитивным и неприводимым, он может быть выбран для построения поля GF(24). Из теории полей Галуа следует, если примитивный полином P1(x)= x4 +x +1 образует поле GF(24), то также примитивным полиномом, образующим изоморфное поле GF(24), будет и двойственный к P1(x) полином x4 P1(x-1) = x4(x–4 +x–1 +1) = 1+x3 + x4= P3(x).

Теперь рассмотрим случай, если был бы выбран для построения поля GF(24) полином P4(x)= x4 + x3 + x2 +x +1. Принимая ε за корень полинома и возводя ε в последовательные степени *i*>0 до появления равенства получим следующий ряд элементов:

|  |
| --- |
| ε |
| ε2 |
| ε3 |
| ε4=1+ε+ε2+ε3 |
| ε5=ε+ε2+ε3+ ε4= =ε+ε2+ε3+ 1+ε+ε2+ε3 =1(mod P4(x)). |

Из таблицы видно, что порядок элемента ε равен *i*=5. Отсюда следует вывод, что полином P4(x) не является примитивным и не может использоваться для построения поля GF(24). Остаётся выяснить, будет ли этот полином неприводимым. Для этого проанализируем значение числа *i* в сравнении ε*i*+1≡0 (mod P4(x)), где Так , равное 5, является делителем числа то полином P4(x), в соответствии со свойством 1.8, входит как сомножитель в разложение на неприводимые сомножители двучлена

=

Это является свидетельством того, что полином P4(x) 4-ой степени является неприводимым, но для построения поля GF(24) он не подходит.

Наконец допустим, что мы выбрали для построения поля P2(x)= x4 +x2 +1. Можем сразу определить, что этот полином не может служить образующим для поля GF(24) так как он, в силу свойства 1.4 полей Галуа, является приводимым, а именно: (x4 +x2 +1)= (x2 +x +1)2.

Но если мы это упустили бы из виду и попытались бы строить поле GF(24), как это, по-видимому, и делал Никита Баталин, путём возведения элемента ε в последовательные степени до 1, то получили бы следующий ряд:

|  |
| --- |
| ε |
| ε2 |
| ε3 |
| ε4=1+ε2 |
| ε5=ε+ε3 |
| ε6=ε2+ ε4= =1+ε2+ε2 =1(mod P2(x)). |

Заметим, что число *i* = 6 , при котором получена 1, не является делителем числа 15. Поэтому полином P2(x) не входит в число сомножителей неприводимых полиномов в разложении двучлена и, следовательно, не является неприводимым.

Таким образом, существуют только два полинома 4-ой степени, пригодных для построения поля GF(24): P1(x)= x4 +x +1 и двойственный к нему полином P3(x)=1+x3 + x4.

Думаю, что для более глубокого познания теории полей Галуа, было бы полезно путём такого же анализа постараться найти для построения поля GF(25) полиномы 5-ой степени.

Если кто-нибудь возьмётся, сообщите мне.

С уважением, Олег Станиславович.

2.03.2021