

Hardware Security
Dr. Debdeep Mukhopadhyay
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture – 11
Field Isomorphisms (Contd.)

So, let us start on the next part of the talk. So, where we shall be discussing about again not continuing about what we were talking in the last class on field isomorphisms. In particular we shall be trying to see how we can construct these transformations in a more algorithmic manner, ok.

(Refer Slide Time: 00:33)

CONCEPTS COVERED

Concepts Covered:

- Isomorphism and Composite Fields
- Construction of Isomorphisms

FREE ONLINE EDUCATION swamyam

So, I shall be starting with you know like defining of course, like as we have seen an isomorphism but also on a term which is called as composite fields, ok. So, and we shall see how we can develop isomorphisms between the composite fields. And as I said like how we can algorithmically construct these isomorphisms, ok. So, I shall state two broad algorithms and the final algorithm is more efficient compared to the first one, ok.

(Refer Slide Time: 01:01)

The slide is titled "Composite Fields" and contains the following text:

- The pair of the fields $GF(2^n)$ and $GF(2^n)^m$ is called a composite field.
- If there exists irreducible polynomials, $Q(Y)$ of degree n and $P(X)$ of degree m , which are used to extend $GF(2)$ to $GF(2^n)$, and $GF(2^n)^m$ from $GF(2^n)$.
- The composite field $GF(2^n)^m$ is isomorphic to the field $GF(2^k)$, where $k = m \times n$.

At the bottom of the slide, there are logos for "THE ONLINE EDUCATION swayam" and "INDIA WISE, LEAD WISE". A video feed of a presenter is visible in the bottom right corner.

So, therefore, what are composite fields? So, as we have seen fields of the or extension fields of the type of GF to the power of n , we can also construct fields of the type of GF of $GF 2$ to the power of n whole power of m . So, these kind of fields are called as composite fields.

So, if there exists irreducible polynomials say $Q Y$ of degree n then I can use that $Q Y$ and construct a field $GF 2$ to the power of n from $GF 2$, and then I use a polynomial $P X$ of degree m , which are used to extend GF I mean $GF 2$ to the power of n to $GF 2$ to the power of n whole power of m , ok. So, therefore, right fine I extend from $GF 2$ to $GF 2$ to the power of n using $Q Y$ and I extend $GF 2$ to the power of n to $GF 2$ to the power of n whole power of m using $P X$.

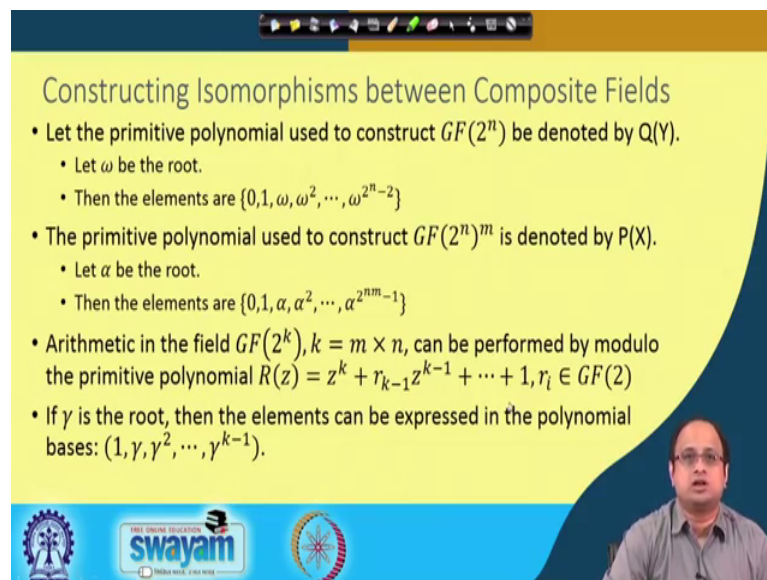
So, now, the composite field which is denoted as $GF 2$ to the power of n whole power of m , you can easily understand that if I consider another field say $GF 2$ to the power of k , where k is equal to m into n that is the product of m and n then the number of elements in $GF 2$ to the power of n whole power of m and $GF 2$ to the power of k are equal, are same they are equinumerous, ok. So, therefore, right if I can establish of a one to one homomorphism between them then that qualifies as an isomorphism. So, I can establish an isomorphism between these fields, I can establish an isomorphism between $GF 2$ to the power k to $GF 2$ to the power of n whole power of m and also vice versa. So, I can

transform an event from this field to this field and also from this field back to GF 2 to the power of k.

So, this can actually give rise or give opportunities or for efficient implementations, where I have got an original field say GF 2 to the power of 8, say k is equal to 8. I transform this into say n equal to 4 and m equal to 2, so I transform this into a field GF 2 to the power of 4 whole square and I do my computations in this field. So, as I will see or we will see in more details in subsequent classes that means, that I can now do the computations right or the fundamental computations in GF 2 to the power of 4 which is a much more simple field compared to GF 2 to the power of 8. And once the result is done in GF 2 to the power of 4 whole square I can get the result back to GF 2 to the power of 8 by using my reverse transformation.

I can do further decompositions; that means, I can decompose GF 2 to the power of 4 further into GF 2 square and I can get a field which is like GF 2 to the power of 2 power of 2 power of 2 which is also, would be isomorphic to GF 2 power of 8, ok.

(Refer Slide Time: 03:41)



The slide is titled "Constructing Isomorphisms between Composite Fields" and contains the following text:

- Let the primitive polynomial used to construct $GF(2^n)$ be denoted by $Q(Y)$.
 - Let ω be the root.
 - Then the elements are $\{0, 1, \omega, \omega^2, \dots, \omega^{2^n-2}\}$
- The primitive polynomial used to construct $GF(2^n)^m$ is denoted by $P(X)$.
 - Let α be the root.
 - Then the elements are $\{0, 1, \alpha, \alpha^2, \dots, \alpha^{2^{nm}-1}\}$
- Arithmetic in the field $GF(2^k)$, $k = m \times n$, can be performed by modulo the primitive polynomial $R(z) = z^k + r_{k-1}z^{k-1} + \dots + 1, r_i \in GF(2)$
- If γ is the root, then the elements can be expressed in the polynomial bases: $(1, \gamma, \gamma^2, \dots, \gamma^{k-1})$.

The slide also features a video feed of a presenter in the bottom right corner and logos for "swayam" and "MHRD" at the bottom.

So, how do we construct isomorphism between composite fields is what we shall study in today's class. So, if you remember like we discussed about primitive polynomials. So, therefore, right these primitive polynomials will be used to construct say GF 2 to the power of n which is denoted as say Q Y, ok.

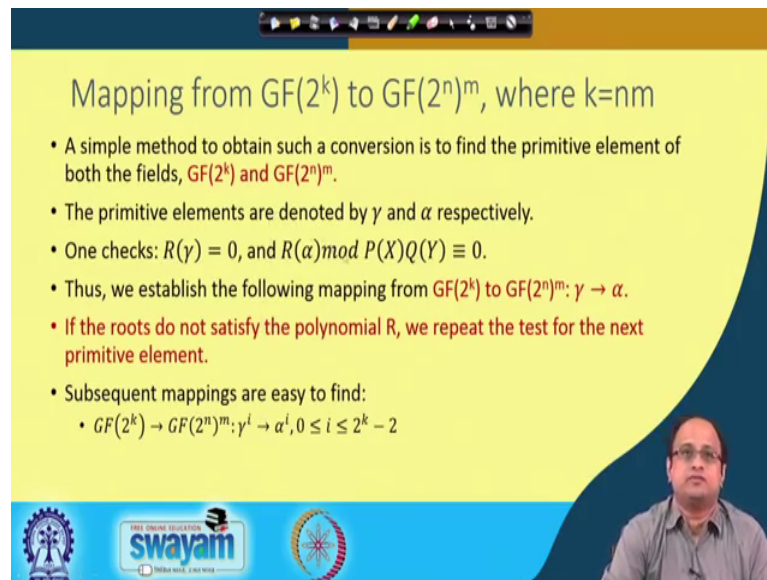
So, note that primitive polynomials are also irreducible as we have discussed. So, therefore, right we they are essentially can be used to extend the field $GF(2)$ to $GF(2^m)$. And suppose ω is the root of this primitive polynomial. So, note that if it is a root then it is also a primitive element. So, therefore, now the elements $0, 1, \omega, \omega^2, \dots, \omega^{n-2}$ will therefore, give all my elements in $GF(2^n)$, ok.

You can think of the example that I gave you for $GF(2^4)$, so that I had all you know like 15 nonzero elements, in a more general setting there will be $2^n - 1$ nonzero elements and of course, you have 0. Likewise, you can also use the primitive polynomial to construct $GF(2^m)$ and as I said we denote it by $P(x)$, ok. So, let α be the root of this and now the elements will be $0, 1, \alpha, \alpha^2, \dots, \alpha^{m-1}$, ok.

So, now, I have got all the elements say in $GF(2^m)$ and there are totally 2^m elements in this in this field. So, now, the arithmetic I want to define arithmetic in the field $GF(2^k)$ which is my original target field, where k is equal to m/n . Now, this can be performed by modulo the primitive polynomial $R(z)$, ok.

So, what is $R(z)$? Now, $R(z)$ is nothing but $z^k + r_{k-1}z^{k-1} + \dots + r_1z + r_0$, where each of this r_i belongs to $GF(2)$; that means, they are either 0, 1 elements. So, again if γ is a root γ is a root of this polynomial then elements can be expressed in the polynomial basis like $1, \gamma, \gamma^2, \dots, \gamma^{k-1}$, in like as we have seen in the previous discussions.

(Refer Slide Time: 05:55)



Mapping from $GF(2^k)$ to $GF(2^n)^m$, where $k=nm$

- A simple method to obtain such a conversion is to find the primitive element of both the fields, $GF(2^k)$ and $GF(2^n)^m$.
- The primitive elements are denoted by γ and α respectively.
- One checks: $R(\gamma) = 0$, and $R(\alpha) \bmod P(X)Q(Y) \equiv 0$.
- Thus, we establish the following mapping from $GF(2^k)$ to $GF(2^n)^m$: $\gamma \rightarrow \alpha$.
- If the roots do not satisfy the polynomial R , we repeat the test for the next primitive element.
- Subsequent mappings are easy to find:
 - $GF(2^k) \rightarrow GF(2^n)^m; \gamma^i \rightarrow \alpha^i, 0 \leq i \leq 2^k - 2$

So, how do I map $GF(2^k)$ to $GF(2^n)^m$ where k is equal to nm ? A very simple method to do this conversion is to find the primitive element of both the fields. So, $GF(2^k)$ and $GF(2^n)^m$ the primitive elements are say γ and α , which means like γ is a primitive element of this field and α is a primitive element of this field, ok.

So, now what I will do is that I will make a check if you remember the example that I gave you exactly like that I will check that of course, like since γ is a primitive element it has to satisfy all of $\gamma^i = 0$ because it is a root of the polynomial $R(x)$, ok. And $R(\alpha)$ that means, this element where I mean I am mapping γ to α , ok. So, therefore, this α should or if I plug in α to R but now I have to do a modulo in the target field, ok. So in the, if you remember in the example it was, I was doing modular F_2 , ok. So, here we have to do modular of $P(X)Q(Y)$ because there are two polynomials on which you have two function. $P(X)$ will be your bigger polynomial, because your essentially this will be of degree m and $Q(Y)$ will be essentially your degree n polynomial which is essentially for working on your base fields or on the subfields, ok.

So, therefore, right if this satisfies then you map γ to α , and if the roots do not satisfy the polynomial we repeat the test for the next primitive element, ok. So, you repeat it for the next primitive element. So, once you have got that map you know

gamma and alpha then you can essentially for all the 2 to the power of k minus 2 elements which are essentially I mean for all the 2 to the power of k minus 1 nonzero elements you can define mappings by just mapping gamma power of i to alpha power of i, ok. So, then in that case you basically map all the elements, ok.

(Refer Slide Time: 07:53)

Algorithm

Input: $n, m, Q(Y), P(X), R(Z)$

Output: $GF(2^k) \rightarrow GF(2^n)^m, k = n \times m$

1. Find primitive elements of $GF(2^k)$: γ
2. For $(\alpha = 1; \alpha < 2^{nm} - 1;)$ do
 if(isPrimitive(α) & $R(\alpha) \bmod Q(Y)P(X) \equiv 0$) break;
 end
3. For $(i=0; i < 2^{nm} - 1; i++)$
 $a_1 = \alpha^i \bmod Q(Y)P(X), b_1 = \gamma^i \bmod R(Z)$
 $b_1 = \gamma^i \bmod R(Z)$
 Map: $a_1 \rightarrow b_1$

So, therefore, the algorithm right for doing, we can actually state this in an algorithmic fashion. So, the input is n and m, Q Y, P X and R z which are my polynomials and I want to map GF 2 power of k to GF 2 power of n whole power of m, where k is equal to n into m. So, we find out the primitive element of GF 2 power of k which is denoted as gamma and for alpha equal to 1 to alpha 2 to the power 2 to the power of n m minus 1; that means, for all the possible elements in GF 2 to the power m n, I have to calculate I have to check this that is whether alpha is a primitive element in my target group and whether it satisfies this equation that is R alpha mod of Q Y, P X is congruent to 0.

The moment I do I get such an element I can break and I essentially have got my alpha and therefore, I can establish my mapping for all the 2 to the power of m n elements, ok. Therefore, I can map I can calculate alpha power of i calculate gamma gamma power of i. Note that in when I am doing calculation alpha power of i, I have to always do modulo of Q Y, P X, and my b 1 essentially is gamma to the power of i mod R z. So, this has been repeated twice but anyway you can just keep it once. So, basically gamma power of

i mod of $R(z)$ and then I map a^{-1} to b^{-1} , basically I map an element a^{-1} to b^{-1} and I get all the possible mappings required. So, let us see an example for that.

(Refer Slide Time: 09:15)

Example: $GF(2^4) \rightarrow GF(2^2)^2$

- $R(Z) = Z^4 + Z + 1, Q(Y) = Y^2 + Y + 1, P(X) = X^2 + X + \{2\}$, where $\{2\} \in GF(2^2)$.
- Note, $Q(Y)$ is used to construct $GF(2^2)$, while $P(X)$ is used to extend to the field $GF(2^2)^2$.
- First primitive element $\gamma \in GF(2^4)$ is 2. It can be checked that '2' can be used to generate all the non-zero elements of $GF(2^4)$.
- Likewise, the first primitive element of $GF(2^2)^2$, st. $R(Z) \equiv 0 \pmod{Q(Y)P(X)}$ is 4.
- Hence, the map is: $\{2\} \rightarrow \{4\}$. Also, 0 is mapped to 0.

So, suppose I said I want to map $GF(2^4)$ to $GF(2^2)^2$, which is a composite field and I said $R(Z)$ as $Z^4 + Z + 1$ my $Q(Y)$ is $Y^2 + Y + 1$ and $P(X)$ is $X^2 + X + 2$. Note that here this polynomial is an irreducible polynomial for $GF(2^2)^2$, ok. So, the elements can be elements from $GF(2^2)$ whereas, these elements are irreducible polynomials respectively for $GF(2^4)$ and this is for $GF(2^2)$. So, the elements are in 0 and 1 in $GF(2)$.

So, note that $Q(Y)$ is used to construct $GF(2^2)$ while $P(X)$ is used to extend to the field $GF(2^2)^2$, ok. So, the first primitive element is say γ which, I mean I mean γ which belongs to $GF(2^4)$ is 2, that is you can also represent it by the polynomial x , because this has got what a minority presentation which is 1 0 and therefore, that stands for x .

Now, it can be checked that 2 can be used to generate all the nonzero elements of $GF(2^4)$, so it is a primitive element. Likewise, the first primitive element of $GF(2^2)^2$ such that this condition that we were checking that is $R(z)$ is congruent to 0 mod of $Q(Y), P(X)$ is true is actually 4, ok. So, 4 would mean that essentially it is 0 1 0 0.

Note that this is an element of GF 2 square square. So, therefore, if I have got an element 0 1 0 0, then that would stand as I mean essentially it means that the first part is 1, and the second part is 0 0, ok. So, there are two parts in the i expansion, ok. So, therefore, right if this is true then I will map 2 to 4, and 0 will get mapped into 0, so all the other elements I will get mapped into say 2 square to 4 square 2 cube to cube and so on, ok. So, in more details, this is a proof that 4 indeed belongs to GF 2 I mean which belongs to GF 2 square; this will be like GF 2 square square, ok; so GF 2 square square is actually indeed the correct choice.

(Refer Slide Time: 11:19)

Example Isomorphic Mapping $GF(2^4) \rightarrow GF(2^2)^2$

Proof that $\{4\} \in GF(2^2)$ is the correct choice.

Note, $\{4\} = 0100 = X$
 $R(X) = X^4 + X + 1 \pmod{Q(Y)P(X)}$
 Note: $X^2 = X + \{2\} \Rightarrow X^3 = 3X + 2 \Rightarrow X^4 = 3X^2 + 2X = 3(X + 2) + 2X = X + 1 \Rightarrow R(4) = 0 \pmod{P(X), Q(Y)}$

$GF(2^4)$	$GF(2^2)^2$	$GF(2^4)$	$GF(2^2)^2$
{02}	{04}	{04}	{06}
{08}	{0e}	{03}	{05}
{06}	{02}	{0c}	{08}
{0b}	{0b}	{05}	{07}
{0a}	{0a}	{07}	{03}
{0e}	{0c}	{0f}	{0d}
{0d}	{09}	{09}	{0f}
{01}	{01}	{00}	{00}

For checking, 3,2 in $GF(2^2)$, express 3 as $Y+1$, and 2 as Y . Thus, with the irreducible polynomial $Q(Y) = Y^2 + Y + 1$, we have $Y(Y+1) = 1$.

Handwritten notes:
 $GF(2^2)^2$
 $\begin{matrix} 1 & 0 \\ a & b \end{matrix}$
 $ax + b, a, b \in GF(2^2)$
 $x^2 = x + \{2\}$
 $x^3 = x^2 + \{2\}x = x + \{2\}x = x + \{2\}x$

So, note that 4 is 0 1 0 0 and therefore, this is nothing this 0 1 is X, and this is 0 0, ok. So, note that this is not an element in GF 2 power of 4. If this was an element in GF 2 power of 4 then this would have been X square, I would have represented as X square, but this is an element of GF 2 square whole square, I missed out this 2 2, here it is actually GF 2 square whole square. So that means, right in GF 2 square whole square let me try to write here.

So, essentially that means, that if I have got you know like an element say GF 2 square whole square, ok. So, it means that the polynomial or the representation is as follows, so that means, like there are two parts of this decomposition the first part is say a, the second part is also b, is b. And therefore, the element is actually ax plus b, where a and b both belongs to GF 2 square, ok so that means, right if I have got and I mean a as 0 1, ok.

So, if I have got a as 1 and b as 0, which are elements in $GF(2)$. Then this is what? This is nothing but X , and that is what we have denoted here as X , ok. So, likewise right, so now, with this with this you know like background you can verify that whether the condition that we had (Refer Time: 13:19) is getting satisfied. So, I calculate $R(X)$ and therefore, $R(X)$ is nothing but $X^4 + X + 1$, ok. And we know that; so now, interesting is that how we do the mod of $Q(Y)P(X)$, ok. So, you note that I have got X to the power of 4 plus X plus 1, and X to the power of 4 plus X plus 1 needs to be reduced. So, therefore, I use first my polynomial which is $P(X)$, ok.

So, in $P(X)$ my polynomial was X^2 equal to $X + 2$ or $X^2 + X + 2$. So, if I set that to 0, I have got X^2 equal to $X + 2$. So, 2 is an element of $GF(2)$. So, therefore, X^3 is equal to if I just you know like cube this, ok. So, I mean I mean if I just multiply this with X then I will get and if I do again at some simplifications. So, note that the moment if I multiply this X^2 with X , ok. So, suppose I have got $X^2 + X + 2$, and if I multiply this by X then I will get $X^3 + 2X$, ok. But note that in this polynomial or in this representation because I am talking about $GF(2)$ whole square X^2 is nothing but $X + 2$. So, therefore, I will replace this with $X + 2$, plus $2X$.

So, therefore, right if I want to calculate this or simplify this further I can take X common and then I add 1 plus 2 that is 1 gets added with 2 plus 2, ok. Now, note this math is essentially again done in $GF(2)$. So, if I want to do 1 plus 2; that means, it is nothing but 0 1 X odd with 1 0, and therefore, I get 1 1 here, and this 1 1 is nothing but 3 and that is why I have got here $3X$, and this two will come here. So, I get $3X + 2$, right.

So, likewise right I calculate X^4 which is $3X^2 + 2X$ make some simplifications I get $X + 1$, ok. So, therefore, right now you can observe that if I get, so therefore, X^2 is equal to $X + 1$, and this implies that R^4 , if I get R^4 and you know like R^4 will be equal to 0 mod $P(X)Q(Y)$ because now I have to bring in $Q(Y)$ into play, and you know and therefore, right I get this as 0, ok. So, therefore, right I mean I mean I get $X + 1$ here which is my X^4 , so if I substitute $X + 1$ here then I get $X + 1 + X + 1$ which is equal to 0, ok. So, therefore, R^4 is indeed equal to 0 mod $P(X)Q(Y)$ and therefore, right my condition is satisfied, ok.

So, therefore, keep in mind that when you are doing computations like 3 into 2 in GF 2 square then you have to express 3 as $Y + 1$, and 2 as Y and therefore, when you are doing computations of say $3Y + 1$ into Y , then you will have Y that that has $Y^2 + Y$ and $Y^2 + Y$ is nothing but 1 because now your polynomial is $Q(Y)$. So, therefore, when you are doing the final step here, ok. So, therefore, this 3 I multiplied with 2 and I you know like wrote 1 over there because 3 into 2 in GF 2 square with this irreducible polynomial is 1, ok. So, this math you have to do little bit in a careful manner, but if we do that then we should be able to easily verify that this equation this is indeed satisfied, ok.

So, with this you know like; so therefore, right I mean let us try to go ahead and try to see. So, there were now once you have you know like got these this checked out you know that 2 gets mapped into 4 you can take the power of 2 and power of 4 and again do you know like similar computations, and you can develop a mapping for all the 15 nonzero elements and I map 0 to 0, ok. So, this is one way in which I can algorithmically develop an isomorphism between these composite fields, ok.

But at the same time, you can easily understand that for this particular construction I was doing an exhaustive analysis, I was doing an analysis. So, if you remember the you know like the for loop counts then you will see that the for loop essentially you know like goes for all possible things that, it goes for all 2^m values, and this is not very efficient when you are trying to do it for larger fields, ok. So, there is an efficient algorithm for handling this. So, let me talk about that subsequently.

(Refer Slide Time: 18:15)

An Efficient Conversion Algorithm

- Present an efficient algorithm between binary and composite fields.
- Maps $GF(2^k) \rightarrow GF(2^m)$, $k = n \times m$
- Returns a binary $k \times k$, 0-1 matrix T , which performs the mapping.
- Evidently, the inverse of T does the reverse mapping.
- The mapping works by relating only k elements (rather than 2^k).
 - It maps the basis vectors.

Handwritten diagrams: $GF(2^k)$ is mapped to $GF(2^m)$ via a $k \times k$ matrix T and a $k \times 1$ vector.

So, here I want to present an efficient algorithm between binary and composite fields, I want to map $GF(2^k)$ again to $GF(2^m)$ where k is equal to $n \times m$ and I want to develop a 0-1 matrix. So, this is the $k \times k$ matrix which means that I can take any $GF(2^k)$ element multiplied with this matrix and I should get back my resultant output, ok. So, again let me try to explain this which means that suppose now I have got t , so this T matrix is now a $k \times k$ matrix. So, this is what I want to construct out of the algorithm, ok.

And I take an element in $GF(2^k)$ and as you know that any $GF(2^k)$ element can be expressed as a vector of dimension k , ok. So, I can express that as a $k \times 1$ vector. So, now, if I multiply this T matrix with this element in say $GF(2^k)$, I get another k dimensional result, but this k dimensional result now should belong to $GF(2^m)$, ok. So, that is the overall objective. So, I want to basically construct this matrix, ok. So, this matrix I mean I mean you know like I will say I will try it of course, like if I can develop this matrix then and if this matrix inverse also exist then the inverse of this matrix will give me the reverse transformation, from $GF(2^m)$ to $GF(2^k)$.

So, the interesting thing is that rather than 2^k which I was doing in the previous algorithm this mapping I can do, I can develop by only mapping k elements which are the basis vectors. I will just map only the basis vectors and that should be

sufficient, ok. So, therefore, right I mean let us see about how we can do that and you know like we should be able to do that in a much more efficient manner.

(Refer Slide Time: 20:13)

The slide is titled "Mapping the k elements" and contains the following text:

- The polynomial bases of $GF(2^k)$ is $\{1, \gamma, \gamma^2, \dots, \gamma^{m-1}\}$, where γ is the primitive element of $GF(2^k)$.
- The unity in both fields is the polynomial 1.
- We first map the unity element in $GF(2^k)$ to the unity element in $GF(2^n)^m$.
- The primitive element in $GF(2^k)$, say γ is mapped to the element α^t , the base element γ^2 is mapped to α^{2t} . Thus continuing, $T(\gamma^i) = \alpha^{it}, i = 0, 1, \dots, k - 1$

The slide also features logos for "swayam" and "INDIA RISE, EDUCATION RISE" at the bottom, and a small video feed of a man in the bottom right corner.

So, what I do here is that I essentially look at my polynomial basis for GF 2 to the power k which is denoted as 1, gamma, gamma square till gamma to the power of m minus 1, where gamma is a primitive element of GF 2 power of k, ok. So, therefore, right I mean now and I find out the unity in both the and I for the first thing which I do is that I map the unity of the both the fields. I map the one in the in the field GF 2 to the power k to GF 2 to the power n whole power of m. Now, the one in both the fields is denoted by the polynomial 1, ok.

So, therefore, right the first we first map the unity element in GF 2 to the power k to the unity element in GF 2 to the power of n whole power of m, and essentially right I mean that means, that I have got one column of my matrix decided, ok. So, I will clarify that. So, then what I do is that I find out the primitive element in GF 2 to the power k, the primitive element which may essentially as we have discussed in your previous discussions. So, I get say that element is denoted as say gamma. So, now, gamma is mapped into alpha power of t, and alpha and which is essentially the base element, ok.

So, now, what I do is that I map I map gamma to alpha power of t, and then I mapped gamma square to alpha power of 2 t and likewise I continue this and I map gamma power of i to alpha power of it, ok. That means, I do this for all k values from 0 to k minus 1 I

do it only for k values, ok. And if I have done that then my entire mapping is decided, ok. So, therefore, if I plug in I equal to 0 that stands for 1. So, I have already mapped 1 into 1 and I start mapping you know like γ power of 1; that means, γ to α power of i , and I mean α power of t and then I mapped γ square t α power of $2t$ and likewise γ to the power of $k-1$ to α to the power of $k-1$, ok. If I have done that then I have mapped all my basis vectors. So, these are my basis vectors, ok. So, maybe you should make a correction here this m will be k , ok.

So, I mapped because in $GF(2^k)$ to the power k there are k basis vectors, ok, there is this m is a wrong yeah wrong thing. So, maybe we should correct it. So, I mapped all the k elements here by this transformation.

(Refer Slide Time: 22:39)

The slide is titled "Check for t" and contains the following text:

- Of course, the choice of t cannot be arbitrary, it has to be done such that the homomorphism is established wrt. additions and multiplications.
- We check, $R(\alpha^t) = 0, \text{ mod } Q(Y)P(X)$.
- There will be exactly k primitive elements which will satisfy the condition, namely α^t and $\alpha^{t2^j}, j = 1, 2, \dots, k-1$. Here the exponents are computed modulo $2^k - 1$. [This follows from the fact that if $R(X) \equiv 0 \Rightarrow R(X^2) \equiv R(X^{2^2}) \equiv 0, j = 1, 2, \dots, k-1$.

The slide also features a video inset of a man speaking in the bottom right corner and logos for "swayam" and "THE OPEN EDUCATION" at the bottom.

So, now I want to check for t because you can easily understand that this choice of t is crucial, because this choice of t will essentially indicate whether the isomorphism property is satisfied. So, again I apply the same trick what I have discussed previously I calculate R α power of t . So, remember that R is my target irreducible polynomial; that means, the irreducible polynomial of my field of my target group, ok. So, therefore, what I do is I mean essentially the; so R is the irreducible polynomial of the field $GF(2^k)$. So, there I plug in α power of t . This should not be 0, but if I do mod of $Q(Y)P(X)$ then I should get 0, exactly in the same way as we have discussed previously.

So, now, there will be exactly k primitive elements which will satisfy this condition. So, this is an important criteria to help us prune and get the choice of t , ok. So, namely you see that if α^t will satisfy this equation then $\alpha^{2^j t}$ will also satisfy this equation where j can go from 1 to $k-1$, ok. So, therefore, note that of course, the exponents are computed modulo $2^k - 1$, ok.

So, why does this result follow? These results follow from this simple observation that if $R(X)$ is congruent to 0 modulo α , I mean its congruent to 0 then in this field because it is a characteristic 2 field $R(X^2)$ is also equal to 0, ok. And likewise, $R(X^{2^j})$ to the power of any 2^j is also equal to 0, ok; that means, for all these $k-1$ values immediately they will also become equal to 0 and if it is not equal to 0 then also these are not equal to 0, ok. And therefore, right we can actually do this that we can we can easily you know like just check this condition, if this condition is not satisfied because if this condition is satisfied then we are done we have got a value of t . But if this is not satisfied then we can immediately rule out some possible t choices, we can actually rule out all these $k-1$ t choices and actually with this all k , we can eliminate t , k t choices at once, ok.

(Refer Slide Time: 24:51)

Algorithm

Input: $n, m, Q(Y), P(X), R(Z)$
Output: T
 α is the primitive element in $GF(2^n)^m$ for which $P(\alpha) \equiv 0$.
 $t=1$
Initialize the array $S[1:2^k-1]$ with 2^k-1 addresses and 1 bit of information.
Initialize a $k \times k$ matrix T with each column indicated by $T[i], 1 \leq i \leq k$
Set $T[k] = (0 \dots 01)^T$
while $(R(\alpha^t) \neq 0)$ {
 for $(j=0; j < k-1; j++)$ $S[t \bmod (2^k-1)] = 0; t++;$
 while $(S[t] = 0 \text{ or } \gcd(t, 2^k-1) > 1)$ $t++;$
}
for $(j=2; j < k; j++)$ $T[j] = \text{binary}(\alpha^{(j-1)t})$

So, in order to do that we actually maintain a data structure which is denoted as an array S , ok; so, this array S essentially stores all the possible values of t , ok. So, there are 2 to

the power of k minus 1 possible values of t . So, I indicate this by an array or with 2 to the power of k minus 1 addresses and 1 bit of information. So, I initialize then this k cross k matrix t which I want to build up with each column indicated by T_i . So, there are k such columns, ok.

Note that interestingly the first column actually is already at least one of the columns is already decided. So, this is what I want to essentially find out. So, note that the k th column essentially means 0 followed by 1 is already decided because I know that 1 should get mapped into 1, ok. So, if I have an element say 1 here that should get mapped into 1, ok. So, therefore, I should get the result also as 1, ok. So, therefore, this essentially means that this column is already known. What we need is the remaining k minus 1 columns, ok. So, in order to know that what we do is a very simple evaluation now is we basically you know like choose t ; that means, we initially started with t equal to 1 and we just you know like and we start with the primitive element in GF 2 to the power of n whole power of m , ok.

So, note that although I have not told in details but there are quite efficient primitive element or primitivity tests which are available, ok. So, we can apply one of them and from there I can you know like verify that whether α is a primitive element or not. You need not you know like generate α and then check you can do it more efficiently, ok. So, therefore, what I do is now I essentially calculate $R \alpha$ power of t and if this is equal to 0 then we are done. So, you can break this while loop, if not then essentially you immediately you can strike out some possible values of S , I mean for some possible values of i by indicated that in indicating that in the S array as 0, ok.

So, now, when you go into the next parts inside the while loop you just check whether S_t is equal to 0 or not because if S_t is equal to 0 then; that means, it has been indicated as not a candidate by a previous run or you check the gcd of t and 2 to the power of k minus 1. Now, you can easily verify that if the gcd of t and 2 to the power of k minus 1 is non-trivial and greater than 1 then t is not a candidate, because t is not in that case essentially that violates its primitivity requirement, ok. And therefore, right you can also you can increment t in that case, ok.

So, therefore, once you have you have passed through this you should get a value of t and once we have got a value of t then what you just do is that for the remaining columns

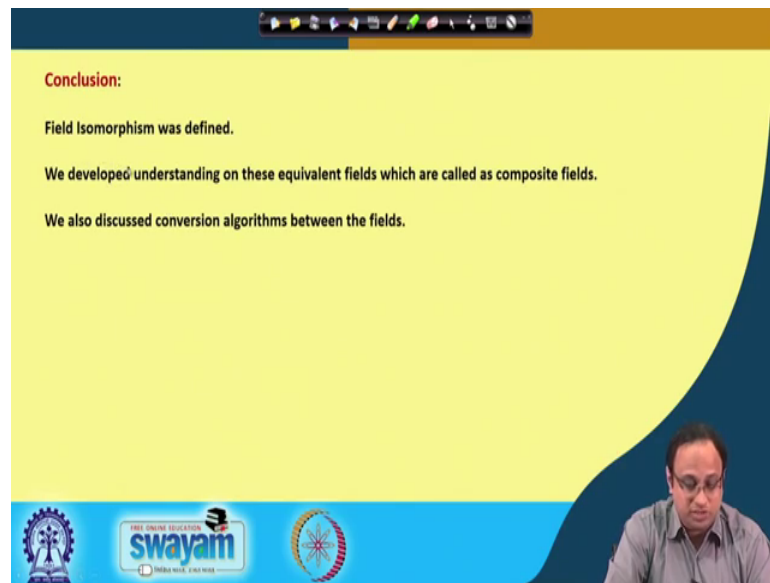
you just write the binary encoding for alpha power of t s, that is alpha power of $2t$, alpha power of $3t$ and so on till alpha to the power of $k-1t$ you just find them and you just write the binary expansion of that, and that will give you this entire matrix, ok.

(Refer Slide Time: 28:01)



So, let me stop here. So, essentially you know like the reference that I have followed is essentially this text, and you should be able to you know like you get more details in the in the book, and I am not really you know like going into all the details but I am trying to give you the major pointers, ok. So, hopefully right I mean you should be able to follow the remaining things from the book.

(Refer Slide Time: 28:31)



Conclusion:

Field Isomorphism was defined.

We developed understanding on these equivalent fields which are called as composite fields.

We also discussed conversion algorithms between the fields.

swamyam
FREE ONLINE EDUCATION
INDIA WISE, LEAD WISE

So, come to conclude. What we discussed in the today's class and also in the last class was we were trying to define field isomorphisms. We tried to develop an understanding on this equivalent fields which are called as composite fields, and we also try to discuss conversion algorithms between the fields, ok like we try to find out efficient mappings between $GF(2^k)$ and $GF(2^m)$. And we shall see you know like in the subsequent classes how we can use this ideas to develop efficient architectures, ok.

Thank you.