② Section 4

18/02/10 Telecoms 2

Equality holds if:

$$\sqrt{S_{nn}(\omega)}\, H(\omega) = K \frac{S^*(\omega) e^{-j\omega T}}{\sqrt{S_{nn}(\omega)}}$$

Now, substituting we obtain:-

$$\left(S/N\right)_o \leq \frac{1}{2\pi} \int_{-\infty}^{\infty} \frac{|S(\omega)|^2}{S_{nn}(\omega)}\, d\omega$$

The max value of $(S/N)_o$ will occur when

$$\boxed{H(\omega) = K \frac{S^*(\omega) e^{-j\omega T}}{S_{nn}(\omega)}}$$

and this is the optimum filter for coloured noise.

Error Correcting Codes:

BCH Codes:

Introduction to Finite Field Theory:

Finite fields belong to abstract algebra. Finite fields are also called "Galois Fields" after Evariste Galois (1811-1832) who discovered them.

A finite field is a set with a finite number of elements along with two operations.

(1) Addition (+)

(2) Multipilication (.)

Let F denote an arbitrary finite field. The operations + and . must satisfy :-

Addition (+)

- Closure, i.e. $a, b \in F$, then $(a+b) \in F$

3

18/02/10 Telecoms 2

cont'd...

- Associativity, i.e. $a, b, c \in F$ then $(a+b)+c = a+(b+c)$
- Commutativity, i.e $a, b \in F$ then;
  $$a+b = b+a$$
- Additive identity element exists. ~~(there)~~ The additive identity element is represented by 0 and satisfies
  $$a+0 = a. \quad a \in F$$
- Additive inverse element exists. for each finite field element i.e. if $a \in F$, then there exists an element $b \in F$ such that:-
  $$a+b = b+a = 0$$

Multiplication:

- Closure $a, b \in F \Rightarrow (a.b) \in F$
- Associativity $a, b, c \in F$ then
  $$(a.b).c = a.(b.c)$$
- Commutativity $a, b \in F$ then
  $$a.b = b.a.$$
- Multiplicative identity element exists and is represented by 1 such that
  $$1.a = a.1 = a \; ; \quad a \in F$$
- Multiplicative inverse element also exist for each finite field element so that if $a \in F$, there exists $b \in F$ such that:-
  $$b.a = a.b = 1$$
- The multiplication operation is distributive over addition: if $a, b, c \in F$, then:
  $$(a+b).c = a.c + b.c.$$

④

8/02/10 Telecoms 2

Finite Field Example:

"work by 5 and keep [illegible]"

Consider {0, 1, 2, 3, 4} along with multiplication and addition performed mod 5

We can denote this field as.

order of field = number of elements in it

GF(5) Galois Field

Consider GF(5) under addition mod 5

Cayley Table

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

(4,4) mod 5 = 8 mod 5 = 3

Consider the Cayley Table for multiplication in GF(5) is:-

•	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

What is the additive inverse of 3, say?
$3 + 2 = 0$ from GF(5) table above.

What is the multiplicitive inverse of 3, say?
$3 \cdot 2 = 1$ from GF(5 table above.

Also 4 is its own multiplicative inverse. $4 \cdot 4 = 1$

19/02/10 Telecoms 2

Constructing Finite Fields:

For every prime number P and integer m, it can be shown that there exists a finite field $GF(p^m)$
Every finite field can be expressed in this form. P is known as the (prime) characteristic of the field.

- $GF(p^m)$ is called an "extension field" of the "base field" $GF(p)$. (see later)

We generally use the base field $GF(2)$ for binary implementation. The binary field $GF(2)$ consists of $\{0,1\}$ with Cayley tables:

mod 2

+	0	1
0	0	1
1	1	0

mod 2

•	0	1
0	0	0
1	0	1

When constructing finite fields, coders/cryptographers etc. generally start with $GF(2)$ and extend it to a new field. To do this, polynomials are used.
If a polynomial $f(x)$ is defined "over a field F" it means that all of its coefficients are taken from the field F.

- An irreducible polynomial is a polynomial that has no factors (or divisors) other that scalars and scalar multiples of itself.
  The irreducibility of a polynomial depends upon the field over which it is defined. (see next section)

We will deal with polynomials over $GF(2)$. (i.e. "binary polynomials")

A Familiar Example

Consider the real number field (albeit an infinite field) and for example, finding the roots of

$$x^2 + 22x + 85 = 0$$

$$\Rightarrow x = -17 \text{ and } x = -5$$

2

19/02/10 Telecons 2

example cont'd.

Now, examine:

$$f(x) = x^2 + 1$$

$$\Rightarrow x = \pm\sqrt{-1} \quad \text{when} \quad f(x) = 0.$$

Even though $f(x)$ is defined over $\mathbb{R}$, it cannot be factored in $\mathbb{R}$. Hence $f(x)$ is irreducible over the field $\mathbb{R}$.

We define a new number i, such that i is a roof of $f(x) \Rightarrow$

$$i = \sqrt{-1}$$

With this definition, we extend $\mathbb{R}$ via the irreducible polynomial $f(x)$ above, to C, the set of complex numbers C is a "new field", consisting of all number of the form $\{a + ib\}$, where $a, b \in \mathbb{R}$. "C is an extension of the base field $\mathbb{R}$."

Similarly, when extending finite fields we:-

1. Define an irreducible polynomial over the base finite field.
2. Let α be the root of the polynomial. α does <u>not</u> belong to the base field, rather it belongs to the extension field.
3. Build the new field with elements in the form $(a + b\alpha + c\alpha^2 + d\alpha^3 \dots)$ where $a, b, c, d \dots \in$ base field.

When adding or multiplying in the extension field, use rules from the base field to compute the coeffs of the α terms. In addition, we use the definition of α (i.e. the eqn with α as a root of the irreducible polynomial to simplify some higher powers of α that might appear.)

3

19/02/10 Telecoms.

$GF(2^3)$

This could be called GF(8) but $GF(2^3)$ is preffered as it explicitly states the base field.

Step 1:

To extend GF(2) to $GF(2^3)$ we need an irreducible polynomial over GF(2). Consider:-

$$f(x) = x^3 + x + 1$$

Coeff $\in \{0,1\}$ note that the degree of $f(x)$, 3, equals the power m in $GF(p^m)$ in $GF(2^3)$, the isn't coincidental...
To confirm $f(x)$ is irreducible over GF(2) evaluate:-

$$f(0) = 1 \quad f(1) = (1^3 + 1 + 1) \bmod 2 = 3 \bmod 2 = 1$$

Hence neither 0 nor 1 is a root of $f(x)$. (Recall $f(\beta) = 0 \Rightarrow \beta$ is a root of the polynomial).

Step 2:

let α b a root of $f(x)$ where $\alpha \in GF(2^3)$. Hence we have:-

$$f(\alpha) = 0$$
$$\Rightarrow \alpha^3 + \alpha + 1 = 0$$
$$\Rightarrow \alpha^3 = \alpha + 1 \quad \text{(addition = subtraction in mod2)}$$

Step 3:

We can build $GF(2^3)$ by considerind linear combinations of α and α^2 terms. Any α^3 terms ~~are~~ or higher power can be replaced via $\alpha^3 = \alpha + 1$.
However it ~~(can be replaced)~~ is easier to build the field by just considering successive powers of α

19/02/10 Telecoms 2

0 (additive identity)
1 (multiplicative identity)
α (a root of the base field irreducible poly)
α^2
$\alpha^3 = \alpha + 1$ (from def of
$\alpha^4 = \alpha(\alpha^3) = \alpha(\alpha+1) = \alpha^2 + \alpha$
$\alpha^5 = \alpha(\alpha^4) = \alpha(\alpha^2 + \alpha) = \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1$
$\alpha^6 = \alpha^2 + 1$ (check)
~~$\alpha^7 = \alpha(\alpha^6) = \alpha^3 + \alpha = 1$~~ already have this.

Hence we have 8 distinct elements. ($GF(2^3)$)
α, in this case, is called a primative element of the field, because one can generate the field by computing successive powers of α and including 0.

$f(x) = x^3 + x + 1$ is called a "primative polynomial" because it has a primative, α, as one of its roots. The irreducible polynomials are not always primative and, hence, their roots may only be able to generate a sub field of the entire finite field.
We can view $GF(2^3)$ in two equivalent ways:-

Exponential Representation	Polynomial Representation
0	0
1	1
α	α
α^2	α^2
α^3	$\alpha + 1$
α^4	$\alpha^2 + \alpha$
α^5	$\alpha^2 + \alpha + 1$
α^6	$\alpha^2 + 1$

25/02/10 Telecoms 2.

$GF(2^4)$ and isomorphism

The polynomial $f(x) = x^4 + x + 1$ will generate $GF(2^4)$. Letting α be a root of $f(x)$, lying in $GF(2^4)$. Since $f(\alpha) = 0$ we have

$$\alpha^4 = \alpha + 1$$

Now, computing successively higher powers of α (and simplifying) generates the following. (See handout)

Since α generates the entire field it is primative and $f(x)$ is a primative polynomial.

Primatives:

Suppose we choose a different element in $GF(2^4)$ and try and generate the field. For example, consider the element α^3 in $GF(2^4)$. Let $\beta = \alpha^3$ for simplicity. Taking powers of β:-

$$\begin{aligned}
\beta^1 &= \alpha^3 \\
\beta^2 &= \alpha^6 \\
\beta^3 &= \alpha^9 \\
\beta^4 &= \alpha^{12} \\
\beta^5 &= \alpha^{15} = \alpha(\alpha^{14}) = \alpha^4 + \alpha = 1 \\
\beta^6 &= \beta\beta^5 = \beta
\end{aligned}$$

The element β. i.e. α^3, is not a primative element.
So, when generating finite fields we prefer to start out with an irreducible polynomial having a primitive as a root.
Tests exist to determine whether a polynomial is irreducible and/or primative. It has been proven that every finite field has at least one primative element
(Note: every element in $GF(2^3)$ is primative)

25/02/10 Telecoms 2

Isomorphism

Any two finite fields with the same number of elements are said to be "isomorphic"
Which means that the fields are essentially the same and differ only in the way the elements are labeled.
For example; let's generate $GF(2^4)$ using a different polynomial

$$p(x) = x^4 + x^3 + x^2 + x + 1$$

$p(x)$ is irreducible over $GF(2)$ but it is not a primative polynomial. If we let α be a root of $p(x)$ we generate:-

α^2

α^3

$\alpha^4 = \alpha^3 + \alpha^2 + \alpha + 1$

$\alpha^5 = \alpha(\alpha^4) = 1$

i.e. $p(x)$ is not a primative polynomial. However, consider

$$y = \alpha + 1$$

and compute $y, y^2, y^3 \cdots y^{15}$. This generates:-

Exponential	Polynomial
0	0
y	$\alpha + 1$
y^2	$\alpha^2 + 1$
y^3	$\alpha^3 + \alpha^2 + \alpha + 1$
⋮	
y^{14}	$\alpha^3 + \alpha$
y^{15}	1.

$(a+b)^2 = a^2 + b^2 + 2ab$ removed by modulo 2

The only way in which this representation differs from the earlier one is that the elements are labeled differently. ↳ cont'd.

(3)

25/02/10 Telecoms 2.

→ cont'd.

So, finite fields with the same number of elements are isomorphic.

⇒ there is only one unique finite field with a given number of elements. (if the fields exist)

Minimal Polynomials:

Preliminary Definition:

If β is an element in $GF(2^m)$, then the conjugates of β are:

$\beta^2, \beta^4, \beta^8 \dots \beta^{2^{r-1}}$, where r is the smallest integer such that $\beta^{2^r} = \beta$

For example, the conjugates of α^3 in $GF(2^4)$ are:-

$$(\alpha^3)^2 = \alpha^6$$
$$(\alpha^3)^4 = \alpha^{12}$$
$$(\alpha^3)^8 = \alpha^{24} = \alpha^{15}\alpha^9 = 1\,\alpha^9 = \alpha^9$$
$$\cancel{(\alpha^3)^{16} = \alpha^{48} = (\alpha^{15})^3 \cdot \alpha^3 = \alpha^3}$$ drop as back to α^3

⇒ conjugates of α^3 are:-

$\alpha^6, \alpha^9, \alpha^{12}$

The minimal polynomial of a field element β is a polynomial consisting of factors of the form $(x+\beta^*)$, where β^* denotes a conjugate of β. Hence, the minimal polynomial of β is:-

$$m(x) = (x+\beta)(x+\beta^2)(x+\beta^4) \dots (x+\beta^{2^{r-1}})$$

The minimal polynomial of element α^i is denoted $m_i(x)$.

For example, in $GF(2^4)$, the minimal polynomial α is:-

$$m_1(x) = (x+\alpha)(x+\alpha^2)(x+\alpha^4)(x+\alpha^8)$$
$$= (x^2+\alpha^5 x+\alpha^3)(x^2+\alpha^5 x+\alpha^{12})$$
$$= x^2 + x + 1)$$

(note: the coeffs in $m_1(x)$ lie in the base field $GF(2)$)

25/02/10 Telecoms 2.

Table of field elements of $GF(2^4)$**: -**

0

1

α

α^2

α^3

$\alpha^4 = \alpha + 1$

$\alpha^5 = \alpha^2 + \alpha$

$\alpha^6 = \alpha^3 + \alpha^2$

$\alpha^7 = \alpha^3 + \alpha + 1$

$\alpha^8 = \alpha^2 + 1$

$\alpha^9 = \alpha^3 + \alpha$

$\alpha^{10} = \alpha^2 + \alpha + 1$

$\alpha^{11} = \alpha^3 + \alpha^2 + \alpha$

$\alpha^{12} = \alpha^3 + \alpha^2 + \alpha + 1$

$\alpha^{13} = \alpha^3 + \alpha^2 + 1$

$\alpha^{14} = \alpha^3 + 1$

25/02/10 Telecoms 2.

It is easy to show, that. the minimal polynomials of α^2, α^4 and α^8 are all equal to $m_1(x)$. It can be shown that, in general;

$$m_i(x) = m_{2i}(x)$$

In relation the coefficients of minimal polynomials, recall the following characteristics of complex numbers:-

If we pick two complex conjugates roots the resulting polynomial has real (~~roots~~) coefficients:

e.g. $2+4i$, $2-4i$ are roots

$\Rightarrow$ minimal poly : $(x-2-4i)(x-2+4i)$

$= x^2 - 4x + 20$ real coeffs

Base - Chaudhuri - Hocquenghem (BCH) Codes:

BCH codes are a subset of the family of cyclic codes. We will consider binary BCH codes. Non-binary BCH codes, although beyond our scope here, are popular in practice:- e.g. Reed- Solomon codes.

Cyclic codes: Recall that any binary word can be represented via a polynomial. For example, consider.

$$\begin{array}{ccccc} 2^4 & 2^3 & 2^2 & 2^1 & 2^0 \\ 1 & 0 & 1 & 1 & 1_2 \end{array}$$

and represent this via

$$x^4 + \cancel{} + x^2 + x + 1$$

Setting $x=2$ would return the decimal value of the original binary number.

05/03/10 Telecoms 2

Example:

Given that $C_1(x)$ and $C_2(x)$ are belonging to the DEC (15,7) code constructed over $GF(2^4)$ incur 2 and 1 errors respectively so giving:-

a) $V_1(x) = x^{11} + x^9 + x^8 + x^6 + x^5 + x + 1$

b) $V_2(x) = x^{12} + x^{11} + x^{10} + x^9 + x^7 + x^5 + x$

respectively determine $e_*(x)$ and $C_*(x)$

Solution

a) The error syndromes are:-

$$S_1 = V_1(\alpha) = \alpha^3 \text{ (after simplification)}$$
$$S_3 = V_1(\alpha^3) = \alpha^{13} \text{ (" ")}$$

over $GF(2^4)$. Substituting into our quadratic yields:-

$$x^2 + x\alpha^3 + \alpha^7 = 0$$

$$\frac{S_1^3 + S_3}{S_1} = \frac{\alpha^9 + \alpha^{13}}{\alpha^3}$$
$$= \alpha^6 + \alpha^{10}$$
$$= \alpha^3 + \cancel{\alpha^2} + \cancel{\alpha^2} + \alpha + 1$$
$$= \alpha^7$$

using table of field elements for $GF(2^4)$

Successively trying field elements for x yields:-

$x = 0$ ✗

$x = 1$ ✗

$x = \alpha$ ✗

⋮ ⋮

$x = \alpha^9$ ✗

$x = \alpha^{10} = X_1$ ✓

Now, $x_2 = S_2 + X_1 = \alpha^3 + \alpha^{10}$
$= \alpha^{12}$

$\Rightarrow e(x) = x^{12} + x^{10}$

2

05/03/'10 Telecoms 2.
cont'd ->

Hence:

$$C_1(x) = V_1(x) + e(x)$$
$$= x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^6 + x^5 + x + 1$$

b)

$$S_1 = \alpha^4 \quad \& \quad S_3 = \alpha^{12}$$

Therefore $S_1^3 + S_3 = \alpha^{12} + \alpha^{12} = 0$

=> our quadratic reduces to:-

$x + \alpha^4 = 0 \Rightarrow X_1 = \alpha^4$

$\Rightarrow e_2(x) = x^4$

$$\Rightarrow C_2(x) = x^{12} + x^{11} + x^{10} + x^9 + x^7 + x^5 + x^4 + x$$

-> Aside:

$$x^2 + S_1 x + \frac{\cancel{S_1^3 + S_3}}{S_1} = 0$$

$$x(x + S_1) = 0$$

$x = 0 \qquad x + S_1 = 0$

"$x=0$" is not permitted since

$X_1 = x^m, m = 0, 1, 2$

$\neq 0$

③

05/03/'10 Telecoms 2.

Consider the (15,7) DEC BCH Code and code word

$$C(x) = x^8 + x^7 + x^6 + x^4 + 1$$

Determine the outcome of a decoder when $C(x)$ incurs the error patterns:-

a) $e(x) = x^7 + x^2 + 1$

b) $e(x) = x^{11} + x^9 + x^6 + x^4$

a)

$$V(x) = C(x) + e(x)$$
$$= x^8 + x^6 + x^4 + x^2$$

giving syndromes:-

$$S_1 = V(\alpha) = \alpha^{11}$$
$$S_3 = V(\alpha^3) = 1$$

over $GF(2^4)$. Substituting into our quadratic yields:-

$$x^2 + \alpha^{11} x + \alpha^3 = 0$$

Trying the field elements in turn shows that no solution exists $\Rightarrow$ decoder concludes that errors occurred but they are not correctable.

b)

Here; $V(x) = x^{11} + x^9 + x^8 + x^7 + 1$

$$\Rightarrow S_1 = V(\alpha) = \alpha^{*}$$
$$S_3 = V(\alpha^3) = 0$$

Trying field elements in turn yields $x = \alpha^2$ as a solution.

$$\Rightarrow X_1 = \alpha^2, \quad X_2 = \alpha^{12}$$
$$\Rightarrow e(x) = x^{12} + x^2$$

but, clearly, we see this is wrong. The decoder, however, will output:

$$C(x) = V(x) + e(x)$$
$$= x^{12} + x^{11} + x^9 + x^8 + x^7 + x^2 + 1$$

which is the wrong code word!

(4)

05/03/10 Telecoms 2

Summer 2008

Q7 (a):
Using $p(x) = x^5 + x^2 + 1$ generate $GF(2^5)$ [9]

$$p(\alpha) = 0 = \alpha^5 + \alpha^2 + 1 = 0$$
$$\Rightarrow \alpha^5 = \alpha^2 + 1$$

0

1

α

α^2

α^3

α^4

$\alpha^5 = \alpha^2 + 1$

$\alpha^6 = \alpha^3 + \alpha$

$\alpha^7 = \alpha^4 + \alpha^2$

$\alpha^8 = \alpha(\alpha^5 + \alpha^3) = \alpha(\alpha^3 + \alpha^2 + 1) = \alpha^4 + \alpha^3 + \alpha$ already multiplied by α

$\alpha^9 = \alpha(\alpha^4 + \alpha^3 + \alpha) = \alpha^4 + \alpha^3 + \alpha^2 + \alpha$

$\alpha^{10} = \cancel{\alpha^2}(\alpha^5)^2 = \alpha^4 + \cancel{\alpha^2}\, 1$

$\alpha^{11} = \alpha^5 + \alpha^3 = \alpha^3 + \alpha^2 + 1$

$\alpha^{12} = \alpha^4 + \alpha^3 + \alpha = \alpha^8$

SEE handout for solution.

b) Show that for the (31, 21) DEC BCH Code based of $GF(2^5)$
(i) Minimal polynomial $m_1(x)$ is given by:
$$m_1(x) = x^5 + x^2 + 1$$ [4]

$$m_1(x) = (x+\alpha)(x+\alpha^2)(x+\alpha^4)(x+\alpha^8)(x+\alpha^{16})$$
since $\alpha^{32} = \alpha^{31}.\alpha = 1.\alpha = \alpha$

$$(x+\alpha)(x+\alpha^2) = x^2 + \alpha^3 + x\alpha^2 + x\alpha = x^2 + x\underbrace{(\alpha^2+\alpha)}_{\alpha^{19}} + \alpha^3$$

$$\Rightarrow x^2 + x\alpha^{19} + x^3$$

David Clowey

05/03/10 Telecoms 2

Given the following table of field elements of $GF(2^5)$: -

0	$\alpha^7 = \alpha^4 + \alpha^2$	$\alpha^{15} = \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$	$\alpha^{23} = \alpha^3 + \alpha^2 + \alpha + 1$
1	$\alpha^8 = \alpha^3 + \alpha^2 + 1$	$\alpha^{16} = \alpha^4 + \alpha^3 + \alpha + 1$	$\alpha^{24} = \alpha^4 + \alpha^3 + \alpha^2 + \alpha$
α	$\alpha^9 = \alpha^4 + \alpha^3 + \alpha$	$\alpha^{17} = \alpha^4 + \alpha + 1$	$\alpha^{25} = \alpha^4 + \alpha^3 + 1$
α^2	$\alpha^{10} = \alpha^4 + 1$	$\alpha^{18} = \alpha + 1$	$\alpha^{26} = \alpha^4 + \alpha^2 + \alpha + 1$
α^3	$\alpha^{11} = \alpha^2 + \alpha + 1$	$\alpha^{19} = \alpha^2 + \alpha$	$\alpha^{27} = \alpha^3 + \alpha + 1$
α^4	$\alpha^{12} = \alpha^3 + \alpha^2 + \alpha$	$\alpha^{20} = \alpha^3 + \alpha^2$	$\alpha^{28} = \alpha^4 + \alpha^2 + \alpha$
$\alpha^5 = \alpha^2 + 1$	$\alpha^{13} = \alpha^4 + \alpha^3 + \alpha^2$	$\alpha^{21} = \alpha^4 + \alpha^3$	$\alpha^{29} = \alpha^3 + 1$
$\alpha^6 = \alpha^3 + \alpha$	$\alpha^{14} = \alpha^4 + \alpha^3 + \alpha^2 + 1$	$\alpha^{22} = \alpha^4 + \alpha^2 + 1$	$\alpha^{30} = \alpha^4 + \alpha$

5

05/03/10 Telecoms 2.

cont'd →

$$(x+\alpha^4)(x+\alpha^8) = x^2 + x\alpha^{14} + \alpha^{12}$$

$$(x^2 + x\alpha^{19} + \alpha^3)(x^2 + x\alpha^{14} + \alpha^{12})(x+\alpha^{16}) = x^5 + x^2 + 1 = m_1(x)$$

conjugates must be 0's or 1's !!

b) (ii)

Show:

$$m_3(x) = x^5 + x^4 + x^3 + x^2 + 1$$

Soln:

$$m_3(x) = (x+\alpha^3)(x+\alpha^6)(x+\alpha^{12})(x+\alpha^{24})(x+\alpha^{48})$$

Since $\alpha^{96} = (\alpha^{32})^3 = \alpha^3$

etc...

b) (iii)

Show that the corresponding generator, $g(x)$, satisfies:

$$g(\alpha) = g(\alpha^3) = 0$$

Soln:

$$g(x) = \text{LCM}[m_1(x), m_3(x)]$$

$= m_1(x)m_3(s)$ since they have no common terms.

$$= \underbrace{(x+\alpha)}_{=0 \text{ if } x=\alpha}(\ldots)\underbrace{(x+\alpha^3)}_{=0 \text{ if } x=\alpha^3}(\ldots)$$