Gabriel Leroux
Paul Troïan

Réalisation d'un QR code

Étape 1 : **Analyse des données à encoder**

On souhaite coder le mot "Hello" dans un qr code, de version 1 et de taux de correction LOW. Selon le tableau ci-après, le nombre maximum de caractères autorisé est 17 pour les binaires.

Version	Modules	ECC Level	Data bits (mixed)	Numeric	Alphanumeric	Binary	Kanji
1	21x21	L	152	41	25	17	10
		M	128	34	20	14	8
		Q	104	27	16	11	7
		H	72	17	10	7	4
2	25x25	L	272	77	47	32	20
		M	224	63	38	26	16
		Q	176	48	29	20	12
		H	128	34	20	14	8
3	29x29	L	440	127	77	53	32
		M	352	101	61	42	26
		Q	272	77	47	32	20
		H	208	58	35	24	15

Étape 2 : **Convertir les caractères de données dans un flux de bytes**

On souhaite maintenant convertir les caractères de données dans un flux de bytes. Pour se faire, nous utilisons, la convention ASCII (voir table ci-dessous) :

"H" : 0100 1000 en binaire => 72 en décimal
"e" : 0110 0101 en binaire => 101 en décimal
"l" : 0110 1100 en binaire => 108 en décimal
"l" : 0110 1100 en binaire => 108 en décimal
"o" : 0110 1111 en binaire => 111 en décimal

ASCII Code: Character to Binary

0	0011 0000	O	0100 1111	m	0110 1101
1	0011 0001	P	0101 0000	n	0110 1110
2	0011 0010	Q	0101 0001	o	0110 1111
3	0011 0011	R	0101 0010	p	0111 0000
4	0011 0100	S	0101 0011	q	0111 0001
5	0011 0101	T	0101 0100	r	0111 0010
6	0011 0110	U	0101 0101	s	0111 0011
7	0011 0111	V	0101 0110	t	0111 0100
8	0011 1000	W	0101 0111	u	0111 0101
9	0011 1001	X	0101 1000	v	0111 0110
A	0100 0001	Y	0101 1001	w	0111 0111
B	0100 0010	Z	0101 1010	x	0111 1000
C	0100 0011	a	0110 0001	y	0111 1001
D	0100 0100	b	0110 0010	z	0111 1010
E	0100 0101	c	0110 0011	.	0010 1110
F	0100 0110	d	0110 0100	,	0010 0111
G	0100 0111	e	0110 0101	:	0011 1010
H	0100 1000	f	0110 0110	;	0011 1011
I	0100 1001	g	0110 0111	?	0011 1111
J	0100 1010	h	0110 1000	!	0010 0001
K	0100 1011	I	0110 1001	'	0010 1100
L	0100 1100	j	0110 1010	"	0010 0010
M	0100 1101	k	0110 1011	(	0010 1000
N	0100 1110	l	0110 1100	)	0010 1001
				space	0010 0000

Avant d'encoder le mot “Hello”, il est important de préciser le type de donnée. Dans notre cas, le message à encoder comporte une majuscule et des minuscules. Par conséquent l’expression binaire commence par 0100, ce qui correspond à l’encoding mode Byte. Le type Byte demande de coder sur 8 bits le nombre de caractères que nous souhaitons. En l'occurrence, “Hello” comporte 5 caractères donc, on obtient 00000101. Ainsi, l'en-tête devient : 0100 00000101.

On ajoute les octets correspondants aux différents caractères de “Hello”, ce qui nous donne : 0100 00000101 01001000 01100101 01101100 01101100 01101111.

Selon le premier tableau, le QR-Code que nous désirons fabriquer est de version 1 et de correction 1, faite pour coder 152 bits, soit 19 octets (152/8). On regroupe par octet, la chaîne binaire ci-avant :
01000000 01010100 10000110 01010110 11000110 11000110 11110000
La partie ocre est ce qu’on appelle un terminator : rajouter des 0 pour compléter l’octet. Nous sommes cependant confrontés à un problème. Notre expression binaire ne fait que 7 octets, elle ne “remplit” pas toute la place disponible, donc il nous faut ajouter encore 12 octets (19-7).

Pour ce faire, il existe deux octets spécifiques 11101100 (Code ASCII 236) et 00010001 (Code ASCII 17) que nous rajoutons l’un après l’autre pour compléter l'entièreté des bits requis. Avant de subir la redondance, notre chaîne binaire devient donc : 01000000 01010100 10000110 01010110 11000110 11000110 11110000 11101100 00010001 11101100 00010001 11101100 00010001 11101100 00010001 11101100 00010001 11101100 00010001.

Étape 3 : **Implémenter la correction des erreurs**

Dans cette étape, on souhaite implémenter la correction des erreurs. Le but est de séparer par blocs les bits de données et de générer leurs codes correcteurs.
Comme vu pour le code de Reed-Solomon, on place un bit d'information et autour, on génère du code correcteur. On s’explique :

Pour commencer il convient de définir l’alphabet sur lequel on travaille. Dans le cas des QR code, on travaille dans GF(256) soit dans 2^8 (On travaille modulo 2).

On a donc $F_{256} = Z_2[x]/(X^8 + X +1)$. On en déduit avec $x=\bar{X}$.

$X^8=X+1$

$X^9=X(X+1)=X^2+X$

$X^{10}=X^3+X^2$

$X^{11}=X^4+X^3$

$X^{12}=X^5+X^4$

$X^{13}=X^6+X^5$

$X^{14}=X^7+X^6$

$X^{15}= X^8+X^7 = X^7+X+1$

$X^{16}=X^8+X^2+X =X^2+2X+1 =X^2+1$

$X^{17}=X^3+X$

$X^{18}=X^4+X^2$

$X^{19}=X^5+X^3$

$X^{20}=X^6+X^4$

$X^{21}=X^7+X^5$

$X^{22}=X^8+X^6 =X^6+X+1$

$X^{23}=X^7+X^2+X$

$X^{24}=X^8+X^3+X^2 =X^3+X^2+X+1$

...

A priori, on n'en a pas fini.

Nous avons donc décidé d'élargir le champ de nos recherches et nous avons trouvé quelque chose d'intéressant : "La spécification du code QR indique d'utiliser l'arithmétique modulo par octet 100011101 (où 100011101 est un nombre binaire équivalent à 285 en décimal). Cela signifie que lorsqu'un nombre est égal ou supérieur à 256, il doit être XORé avec 285. Cela conduit à des valeurs inattendues pour 2^8 et plus. En d'autres termes :

2^8 = 256 ^ 285 = 29".

Autrement dit, nous nous sommes trompés de polynôme irréductible. Ce n'est pas $X^8 + X +1$ mais bel et bien $X^8 + X^4 + X^3 + X^2 +1$. Il convient maintenant de corriger le tir.

Comme nous sommes en base 2, X=2, X^3*X^2 devient $2^3*2^2 = 2^5$. En théorie on calcule toutes les valeurs de X^x avec 0 =< x <=255 puis comme on utilise GF (256) dès que l'exposant est strictement supérieur à 255 on utilise le modulo. Par exemple, si on doit calculer X^{355} on fait $X^{(255+100)}$ modulo 255 ce qui donne X^{100}. Nous avons trouvé une table recensant les puissances de α avec leur correspondance en décimale.

Logarithm table for GF(256) with primitive, irreducible polynomial 285 (0x11D)

by Cody Planteen; https://codyplanteen.com/notes/rs; July 25, 2019

$F(x) = x^8 + x^4 + x^3 + x^2 + 1$, minimum primitive element $\alpha = x = 2$

Example: $35 \cdot 36 = \alpha^{47}\alpha^{225} = \alpha^{272} = \alpha^{272 \bmod 255} = \alpha^{17} = 152$

α^j	j	α^j	j	α^j	j	α^j	j	α^j	j	α^j	j	α^j	j
0	*	37	36	74	37	111	61	148	38	185	60	222	62
1	0	38	15	75	179	112	202	149	184	186	57	223	90
2	1	39	33	76	16	113	94	150	180	187	83	224	203
3	25	40	53	77	145	114	155	151	124	188	71	225	89
4	2	41	147	78	34	115	159	152	17	189	109	226	95
5	50	42	142	79	136	116	10	153	68	190	65	227	176
6	26	43	218	80	54	117	21	154	146	191	162	228	156
7	198	44	240	81	208	118	121	155	217	192	31	229	169
8	3	45	18	82	148	119	43	156	35	193	45	230	160
9	223	46	130	83	206	120	78	157	32	194	67	231	81
10	51	47	69	84	143	121	212	158	137	195	216	232	11
11	238	48	29	85	150	122	229	159	46	196	183	233	245
12	27	49	181	86	219	123	172	160	55	197	123	234	22
13	104	50	194	87	189	124	115	161	63	198	164	235	235
14	199	51	125	88	241	125	243	162	209	199	118	236	122
15	75	52	106	89	210	126	167	163	91	200	196	237	117
16	4	53	39	90	19	127	87	164	149	201	23	238	44
17	100	54	249	91	92	128	7	165	188	202	73	239	215
18	224	55	185	92	131	129	112	166	207	203	236	240	79
19	14	56	201	93	56	130	192	167	205	204	127	241	174
20	52	57	154	94	70	131	247	168	144	205	12	242	213
21	141	58	9	95	64	132	140	169	135	206	111	243	233
22	239	59	120	96	30	133	128	170	151	207	246	244	230
23	129	60	77	97	66	134	99	171	178	208	108	245	231
24	28	61	228	98	182	135	13	172	220	209	161	246	173
25	193	62	114	99	163	136	103	173	252	210	59	247	232
26	105	63	166	100	195	137	74	174	190	211	82	248	116
27	248	64	6	101	72	138	222	175	97	212	41	249	214
28	200	65	191	102	126	139	237	176	242	213	157	250	244
29	8	66	139	103	110	140	49	177	86	214	85	251	234
30	76	67	98	104	107	141	197	178	211	215	170	252	168
31	113	68	102	105	58	142	254	179	171	216	251	253	80
32	5	69	221	106	40	143	24	180	20	217	96	254	88
33	138	70	48	107	84	144	227	181	42	218	134	255	175
34	101	71	253	108	250	145	165	182	93	219	177		
35	47	72	226	109	133	146	153	183	158	220	187		
36	225	73	152	110	186	147	119	184	132	221	204		

Table des log/antilog dans GF(256), avec le polynôme irréductible 285

Nous avons besoin de deux polynômes pour effectuer la division polynomiale afin d'obtenir le code erreur. L'un est appelé "the message polynomial". Il utilise les données à encoder comme coefficient. Dans notre cas, le polynôme message est, en convertissant en décimal les différents octets de notre chaîne binaire :

$m(x)=64x^{18}+84x^{17}+134x^{16}+86x^{15}+198x^{14}+198x^{13}+240x^{12}+236x^{11}+17x^{10}+236x^{9}+17x^{8}+236x^{7}+17x^{6}+236x^{5}+17x^{4}+236x^{3}+17x^{2}+236x+17$

On passe maintenant au polynôme générateur. On sait que la capacité de correction **t**, d'un QR code de version et de redondance **L** est 7. Par conséquent le polynôme générateur est (on ne détaille pas les calculs par soucis de place et de simplicité, on applique simplement la distributivité à l'aide de la table ci-dessus) :

$g(x)=\alpha^{0}x^{7} + \alpha^{87}x^{6} + \alpha^{229}x^{5} + \alpha^{146}x^{4} + \alpha^{149}x^{3} + \alpha^{238}x^{2} + \alpha^{102}x + \alpha^{21.}$

Nous allons maintenant effectuer la division du polynôme message par le polynôme générateur. Nous allons procéder en 3 grandes étapes. La première est de trouver le terme approprié avec lequel on multiplie le polynôme générateur. Le but étant de supprimer le terme de plus haut degré du polynôme message (cf. division polynomiale). La deuxième, logiquement, est donc de soustraire le résultat au polynôme/XOR le résultat avec le polynôme message (car on est dans GF(256) soustraction = XOR). Nous devons répéter ces deux étapes le même nombre de fois qu'il y a de codeword dans le polynôme message. Dans notre cas, nous avons 19 fois car nous avons 19 octets (1 octet = 1 codeword).

Le plus important de ces étapes est de bien comprendre qu'après la division des deux polynômes, il y aura un reste dont les coefficients constitueront le code erreurs des codewords.

Nous développons les 3 étapes de calculs présentés ci-dessus, ci-dessous.

Pour nous assurer que l'exposant du terme principal ne devienne pas trop petit lors de la division on multiplie le polynôme message par x^7 (avec 7 la capacité de correction). Cela nous donne donc :

$m(x)=64x^{25}+84x^{24}+134x^{23}+86x^{22}+198x^{21}+198x^{20}+240x^{19}+236x^{18}+17x^{17}+236x^{16}+17x^{15}+$
$236x^{14}+17x^{13}+236x^{12}+17x^{11}+236x^{10}+17x^{9}+236x^{8}+17x^{7}$.

Le terme principal du polynôme générateur doit également avoir le même exposant, il faut donc le multiplier par x^{18} (le terme de plus haut degré était x^7 : $x^{18}+x^7=x^{25}$).

$g(x)=\alpha^0x^{25} + \alpha^{87}x^{24} + \alpha^{229}x^{23} + \alpha^{146}x^{22} + \alpha^{149}x^{21} + \alpha^{238}x^{20} + \alpha^{102}x^{19} + \alpha^{21}x^{18}$

<u>1/</u> La première étape de la division consiste à multiplier le polynôme générateur par le terme de plus haut degré du polynôme message, en l'occurrence $64x^{25}$. Pour faciliter nos calculs nous allons convertir les coefficients décimaux en puissance alpha :

$m(x)=\alpha^6x^{25}+\alpha^{143}x^{24}+\alpha^{99}x^{23}+\alpha^{219}x^{22}+\alpha^{164}x^{21}+\alpha^{164}x^{20}+\alpha^{79}x^{19}+\alpha^{122}x^{18}+\alpha^{100}x^{17}+\alpha^{122}x^{16}+\alpha^{100}x^{15}+\alpha^{122}x^{14}$
$+$
$\alpha^{100}x^{13}+\alpha^{122}x^{12}+\alpha^{100}x^{11}+\alpha^{122}x^{10}+\alpha^{100}x^{9}+\alpha^{122}x^{8}+\alpha^{100}x^{7}$

Dans notre cas, $64=\alpha^6$ selon la table log/antilog. Cela nous donne donc :

$g(x)=\alpha^6x^{25} + \alpha^{93}x^{24} + \alpha^{235}x^{23} + \alpha^{152}x^{22} + \alpha^{155}x^{21} + \alpha^{244}x^{20} + \alpha^{108}x^{19} + \alpha^{27}x^{18}$
$=64x^{25} + 182x^{24} + 235x^{23} + 73x^{22} + 114x^{21} + 250x^{20} + 208x^{19} + 12x^{18}$

On XOR le résultat obtenu avec le polynôme message.

On a donc : $0x^{25}+ (182 \text{ XOR } 84)x^{24}+ (235 \text{ XOR } 134)x^{23}+ (73 \text{ XOR } 86)x^{22} +$
$(114 \text{ XOR } 198)x^{21}+(250 \text{ XOR } 198)x^{20}+ (208 \text{ XOR } 240)x^{19}+ (12 \text{ XOR } 236)x^{18}$
$+17x^{17}+236x^{16}+17x^{15}+236x^{14}+17x^{13}+236x^{12}+17x^{11}+236x^{10}+17x^{9}+236x^{8}+17x^{7}$

$= 226x^{24}+109x^{23}+31x^{22}+180x^{21}+60x^{20}+32x^{19}+224x^{18}+17x^{17}+236x^{16}+17x^{15}+236x^{14}+17x^{13}+$
$236x^{12}+17x^{11}+236x^{10}+17x^{9}+236x^{8}+17x^{7}$

2/ De même on prend le coefficient du terme le plus haut degré de notre précédent calcul et on multiplie ce dernier au polynôme générateur. Selon la table des log/antilog dans GF(256) $226=\alpha^{95}$: $g(x)= \alpha^{95}x^{24} + \alpha^{182}x^{23} + \alpha^{(324\%255)=69}x^{22} + \alpha^{241}x^{21} + \alpha^{244}x^{20} + \alpha^{(333\%255)=78}x^{19} + \alpha^{197}x^{18} + \alpha^{116}x^{17}= 226x^{24} + 98x^{23} + 47x^{22} + 88x^{21} + 250x^{20} + 120x^{19} + 141x^{18} + 248x^{17}$
On XOR le résultat obtenu avec le polynôme trouvé à la fin de la première étape.
On a donc :
$= 0x^{24}+15x^{23}+48x^{22}+236x^{21}+198x^{20}+88x^{19}+109x^{18}+233x^{17}+236x^{16}+17x^{15}+236x^{14}+17x^{13}+ 236x^{12}+17x^{11}+236x^{10}+17x^{9}+236x^{8}+17x^{7}$

3/ De même on prend le coefficient du terme le plus haut degré de notre précédent calcul et on multiplie ce dernier au polynôme générateur. Selon la table des log/antilog dans GF(256) $15=\alpha^{75}$: $g(x)= \alpha^{75}x^{23} + \alpha^{162}x^{22} + \alpha^{(304\%255)=49}x^{21} + \alpha^{221}x^{20} + \alpha^{224}x^{19} + \alpha^{(313\%255)=58}x^{18} + \alpha^{177}x^{17}+ \alpha^{96}x^{16}= 15x^{23} + 191x^{22} + 140x^{21} + 69x^{20} + 18x^{19} + 105x^{18} + 219x^{17} + 217x^{16}$
On XOR le résultat obtenu avec le polynôme trouvé à la fin de la deuxième étape.
On a donc :
$= 0x^{23}+143x^{22}+96x^{21}+131x^{20}+74x^{19}+4x^{18}+50x^{17}+53x^{16}+17x^{15}+236x^{14}+17x^{13}+ 236x^{12}+17x^{11}+236x^{10}+17x^{9}+236x^{8}+17x^{7}$

4/ De même on prend le coefficient du terme le plus haut degré de notre précédent calcul et on multiplie ce dernier au polynôme générateur. Selon la table des log/antilog dans GF(256) $143=\alpha^{24}$: $g(x)= \alpha^{24}x^{22} + \alpha^{111}x^{21} + \alpha^{253}x^{20} + \alpha^{170}x^{19} + \alpha^{173}x^{18} + \alpha^{(262\%255)=7}x^{17}+ \alpha^{126}x^{16}+ \alpha^{45}x^{15}= 143x^{22} + 206x^{21} + 71x^{20} + 215x^{19} + 246x^{18} + 128x^{17} + 102x^{16} +193x^{15}$
On XOR le résultat obtenu avec le polynôme trouvé à la fin de la troisième étape.
On a donc :
$= 0x^{22}+174x^{21}+196x^{20}+157x^{19}+242x^{18}+178x^{17}+83x^{16}+208x^{15}+236x^{14}+17x^{13}+ 236x^{12}+17x^{11}+236x^{10}+17x^{9}+236x^{8}+17x^{7}$

5/ De même on prend le coefficient du terme le plus haut degré de notre précédent calcul et on multiplie ce dernier au polynôme générateur. Selon la table des log/antilog dans GF(256) $174=\alpha^{190}$: $g(x)= \alpha^{190}x^{21} + \alpha^{(277\%255)=22}x^{20} + \alpha^{(419\%255)=164}x^{19} + \alpha^{(336\%255)=81}x^{18} + \alpha^{(339\%255)=84}x^{17}+ \alpha^{(428\%255)=173}x^{16}+ \alpha^{(292\%255)=37}x^{15}+ \alpha^{211}x^{14}= 174x^{21} + 234x^{20} + 198x^{19} + 231x^{18} + 107x^{17} + 246x^{16} +74x^{15} + 178x^{14}$
On XOR le résultat obtenu avec le polynôme trouvé à la fin de la quatrième étape.
On a donc :
$= 0x^{21}+46x^{20}+91x^{19}+21x^{18}+217x^{17}+165x^{16}+154x^{15}+94x^{14}+17x^{13}+ 236x^{12}+17x^{11}+236x^{10}+17x^{9}+236x^{8}+17x^{7}$

6/ De même on prend le coefficient du terme le plus haut degré de notre précédent calcul et on multiplie ce dernier au polynôme générateur. Selon la table des log/antilog dans GF(256) $46=\alpha^{130}$: $g(x)= \alpha^{130}x^{20} + \alpha^{217}x^{19} + \alpha^{(359\%255)=104}x^{18} + \alpha^{21}x^{17}+ \alpha^{24}x^{16}+ \alpha^{(368\%255)=113}x^{15}+ \alpha^{232}x^{14}+ \alpha^{151}x^{13} = 46x^{20} + 155x^{19} + 13x^{18} + 117x^{17} + 143x^{16} +31x^{15} + 247x^{14}+ 170x^{13}$
On XOR le résultat obtenu avec le polynôme trouvé à la fin de la cinquième étape.
On a donc :
$= 0x^{20}+192x^{19}+24x^{18}+172x^{17}+42x^{16}+133x^{15}+169x^{14}+187x^{13}+ 236x^{12}+17x^{11}+236x^{10}+17x^{9}+236x^{8}+17x^{7}$

7/ De même on prend le coefficient du terme le plus haut degré de notre précédent calcul et on multiplie ce dernier au polynôme générateur. Selon la table des log/antilog dans GF(256) $192=\alpha^{31}$: $g(x)= \alpha^{31}x^{19} + \alpha^{118}x^{18} + \alpha^{5}x^{17}+ \alpha^{177}x^{16}+ \alpha^{180}x^{15}+ \alpha^{14}x^{14}+ \alpha^{133}x^{13}+ \alpha^{52}x^{12} = 192x^{19} + 199x^{18} + 32x^{17} + 219x^{16} + 150x^{15} +19x^{14} + 109x^{13}+ 20x^{12}$
On XOR le résultat obtenu avec le polynôme trouvé à la fin de la sixième étape.
On a donc :
$= 0x^{19}+223x^{18}+140x^{17}+241x^{16}+19x^{15}+186x^{14}+214x^{13}+248x^{12}+17x^{11}+236x^{10}+17x^{9}+236x^{8}+17x^{7}$

8/ De même on prend le coefficient du terme le plus haut degré de notre précédent calcul et on multiplie ce dernier au polynôme générateur. Selon la table des log/antilog dans GF(256) $223=\alpha^{90}$: $g(x)= \alpha^{90}x^{18} + \alpha^{177}x^{17}+ \alpha^{64}x^{16}+ \alpha^{236}x^{15}+ \alpha^{239}x^{14}+ \alpha^{73}x^{13}+ \alpha^{192}x^{12} + \alpha^{111}x^{11} = 223x^{18} + 219x^{17} + 95x^{16} + 203x^{15} +22x^{14} + 202x^{13}+ 130x^{12}+ 206x^{11}$
On XOR le résultat obtenu avec le polynôme trouvé à la fin de la septième étape.
On a donc :
$= 0x^{18}+87x^{17}+174x^{16}+216x^{15}+172x^{14}+28x^{13}+122x^{12}+223x^{11}+236x^{10}+17x^{9}+236x^{8}+17x^{7}$

9/ De même on prend le coefficient du terme le plus haut degré de notre précédent calcul et on multiplie ce dernier au polynôme générateur. Selon la table des log/antilog dans GF(256) $87=\alpha^{189}$: $g(x)= \alpha^{189}x^{17}+ \alpha^{21}x^{16}+ \alpha^{163}x^{15}+ \alpha^{80}x^{14}+ \alpha^{83}x^{13}+ \alpha^{172}x^{12} + \alpha^{36}x^{11} + \alpha^{210}x^{10}$
$= 87x^{17} + 217x^{16} + 99x^{15} +253x^{14} + 187x^{13}+ 123x^{12}+ 37x^{11}+ 89x^{10}$
On XOR le résultat obtenu avec le polynôme trouvé à la fin de la huitième étape.
On a donc :
$= 0x^{17}+219x^{16}+187x^{15}+81x^{14}+167x^{13}+1x^{12}+250x^{11}+181x^{10}+17x^{9}+236x^{8}+17x^{7}$

10/ De même on prend le coefficient du terme le plus haut degré de notre précédent calcul et on multiplie ce dernier au polynôme générateur. Selon la table des log/antilog dans GF(256) $219=\alpha^{177}$: $g(x)= \alpha^{177}x^{16}+ \alpha^{9}x^{15}+ \alpha^{151}x^{14}+ \alpha^{68}x^{13}+ \alpha^{71}x^{12} + \alpha^{160}x^{11} + \alpha^{24}x^{10}+ \alpha^{198}x^{9}$
$= 219x^{16} + 58x^{15} +170x^{14} + 153x^{13}+ 188x^{12}+ 230x^{11}+ 143x^{10}+7x^{9}$
On XOR le résultat obtenu avec le polynôme trouvé à la fin de la neuvième étape.
On a donc :
$= 0x^{16}+129x^{15}+251x^{14}+62x^{13}+189x^{12}+28x^{11}+58x^{10}+22x^{9}+236x^{8}+17x^{7}$

11/ De même on prend le coefficient du terme le plus haut degré de notre précédent calcul et on multiplie ce dernier au polynôme générateur. Selon la table des log/antilog dans GF(256) $129=\alpha^{112}$: $g(x)= \alpha^{112}x^{15}+ \alpha^{199}x^{14}+ \alpha^{86}x^{13}+ \alpha^{3}x^{12} + \alpha^{6}x^{11} + \alpha^{95}x^{10}+ \alpha^{214}x^{9} + \alpha^{133}x^{8}$
$= 129x^{15} +14x^{14} + 177x^{13}+ 8x^{12}+ 64x^{11}+ 226x^{10}+249x^{9} + 109x^{8}$
On XOR le résultat obtenu avec le polynôme trouvé à la fin de la dixième étape.
On a donc :
$= 0x^{15}+245x^{14}+143x^{13}+181x^{12}+92x^{11}+216x^{10}+239x^{9}+129x^{8}+17x^{7}$

12/ De même on prend le coefficient du terme le plus haut degré de notre précédent calcul et on multiplie ce dernier au polynôme générateur. Selon la table des log/antilog dans GF(256) $245=\alpha^{231}$: $g(x)= \alpha^{231}x^{14}+ \alpha^{63}x^{13}+ \alpha^{205}x^{12} + \alpha^{122}x^{11} + \alpha^{125}x^{10}+ \alpha^{214}x^{9} + \alpha^{78}x^{8}+\alpha^{252}x^{7}$
$= 245x^{14} + 161x^{13}+ 167x^{12}+ 236x^{11}+ 51x^{10}+249x^{9} + 120x^{8} + 173x^{7}$
On XOR le résultat obtenu avec le polynôme trouvé à la fin de la onzième étape.

On a donc :
$= 0x^{14}+46x^{13}+18x^{12}+176x^{11}+235x^{10}+22x^{9}+249x^{8}+188x^{7}$

13/ De même on prend le coefficient du terme le plus haut degré de notre précédent calcul et on multiplie ce dernier au polynôme générateur. Selon la table des log/antilog dans GF(256) $46=\alpha^{130}$: $g(x)= \alpha^{130}x^{13}+ \alpha^{217}x^{12} + \alpha^{104}x^{11} + \alpha^{21}x^{10}+ \alpha^{24}x^{9} + \alpha^{113}x^{8}+\alpha^{232}x^{7}+\alpha^{151}x^{6}$
$= 46x^{13}+ 155x^{12}+ 13x^{11}+ 117x^{10}+143x^{9} + 31x^{8} + 247x^{7}+170x^{6}$
On XOR le résultat obtenu avec le polynôme trouvé à la fin de la douzième étape.
On a donc :
$= 0x^{13}+137x^{12}+189x^{11}+158x^{10}+153x^{9}+230x^{8}+75x^{7}+170x^{6}$

14/ De même on prend le coefficient du terme le plus haut degré de notre précédent calcul et on multiplie ce dernier au polynôme générateur. Selon la table des log/antilog dans GF(256) $137=\alpha^{74}$: $g(x)= \alpha^{74}x^{12} + \alpha^{161}x^{11} + \alpha^{48}x^{10}+ \alpha^{220}x^{9} + \alpha^{223}x^{8}+\alpha^{57}x^{7}+\alpha^{176}x^{6}+ \alpha^{95}x^{5}$
$= 137x^{12}+ 209x^{11}+ 70x^{10}+172x^{9} + 9x^{8} + 186x^{7}+227x^{6} + 226x^{5}$
On XOR le résultat obtenu avec le polynôme trouvé à la fin de la treizième étape.
On a donc :
$= 0x^{12}+108x^{11}+216x^{10}+53x^{9}+239x^{8}+241x^{7}+73x^{6}+ 226x^{5}$

15/ De même on prend le coefficient du terme le plus haut degré de notre précédent calcul et on multiplie ce dernier au polynôme générateur. Selon la table des log/antilog dans GF(256) $108=\alpha^{250}$: $g(x)= \alpha^{250}x^{11} + \alpha^{82}x^{10}+ \alpha^{224}x^{9} + \alpha^{141}x^{8}+\alpha^{144}x^{7}+\alpha^{233}x^{6}+ \alpha^{97}x^{5}+\alpha^{16}x^{4}$
$= 108x^{11}+ 211x^{10}+18x^{9} + 21x^{8} + 168x^{7}+243x^{6} + 175x^{5}+76x^{4}$
On XOR le résultat obtenu avec le polynôme trouvé à la fin de la quatorzième étape.
On a donc :
$= 0x^{11}+11x^{10}+39x^{9}+250x^{8}+89x^{7}+186x^{6}+ 77x^{5}+76x^{4}$

16/ De même on prend le coefficient du terme le plus haut degré de notre précédent calcul et on multiplie ce dernier au polynôme générateur. Selon la table des log/antilog dans GF(256) $11=\alpha^{238}$: $g(x)= \alpha^{238}x^{10}+ \alpha^{70}x^{9} + \alpha^{212}x^{8}+\alpha^{129}x^{7}+\alpha^{132}x^{6}+ \alpha^{221}x^{5}+\alpha^{85}x^{4} + \alpha^{4}x^{3}$
$= 11x^{10}+ 94x^{9} + 121x^{8} + 23x^{7}+184x^{6} + 69x^{5}+214x^{4} + 16x^{3}$
On XOR le résultat obtenu avec le polynôme trouvé à la fin de la quinzième étape.
On a donc :
$= 0x^{10}+121x^{9}+131x^{8}+78x^{7}+2x^{6}+ 8x^{5}+154x^{4} + 16x^{3}$

17/ De même on prend le coefficient du terme le plus haut degré de notre précédent calcul et on multiplie ce dernier au polynôme générateur. Selon la table des log/antilog dans GF(256) $121=\alpha^{212}$: $g(x)= \alpha^{212}x^{9} + \alpha^{44}x^{8}+\alpha^{186}x^{7}+\alpha^{103}x^{6}+ \alpha^{106}x^{5}+\alpha^{195}x^{4} + \alpha^{59}x^{3} + \alpha^{233}x^{2}$
$= 121x^{9} + 238x^{8} + 110x^{7}+ 136x^{6} + 52x^{5}+ 100x^{4} + 210x^{3} + 243x^{2}$
On XOR le résultat obtenu avec le polynôme trouvé à la fin de la seizième étape.
On a donc :
$= 0x^{9}+109x^{8}+32x^{7}+138x^{6}+ 60x^{5}+254x^{4} + 194x^{3} +243x^{2}$

18/ De même on prend le coefficient du terme le plus haut degré de notre précédent calcul et on multiplie ce dernier au polynôme générateur. Selon la table des log/antilog dans GF(256) $109=\alpha^{133}$: $g(x)= \alpha^{133}x^{8}+\alpha^{220}x^{7}+\alpha^{107}x^{6}+ \alpha^{24}x^{5}+\alpha^{27}x^{4} + \alpha^{116}x^{3} + \alpha^{235}x^{2}+ \alpha^{154}x$

$= 109x^8 + 172x^7 + 104x^6 + 143x^5 + 12x^4 + 248x^3 + 235x^2 + 57x$
On XOR le résultat obtenu avec le polynôme trouvé à la fin de la dix-septième étape.
On a donc :
$= 0x^8 + 140x^7 + 226x^6 + 179x^5 + 242x^4 + 58x^3 + 24x^2 + 57x$

<u>19/</u> De même on prend le coefficient du terme le plus haut degré de notre précédent calcul et on multiplie ce dernier au polynôme générateur. Selon la table des log/antilog dans GF(256) $140 = \alpha^{49}$: $g(x) = \alpha^{49}x^7 + \alpha^{136}x^6 + \alpha^{23}x^5 + \alpha^{195}x^4 + \alpha^{198}x^3 + \alpha^{32}x^2 + \alpha^{151}x + \alpha^{70}$
$= 140x^7 + 79x^6 + 201x^5 + 100x^4 + 7x^3 + 157x^2 + 170x + 94$
On XOR le résultat obtenu avec le polynôme trouvé à la fin de la dix-huitième étape.
On a donc :
$= 0x^7 + 173x^6 + 122x^5 + 150x^4 + 61x^3 + 133x^2 + 147x + 94$

La division a été faite 19 fois, ce qui correspond au nombre de termes du polynôme message. Cela signifie donc que la division est terminée et que les coefficient des termes en x constituent le code erreur des codewords à utiliser sur le polynôme message original, à savoir : 173 122 150 61 133 147 94.

Maintenant que nous connaissons le polynôme message et le code erreur de ce dernier, nous pouvons nous tourner vers la création concrète du QR code.

<u>Étape 4 :</u> **Insérer les données avec le code correcteur dans la matrice**

On retranscrit en binaire le code correcteur pour ensuite l'insérer dans la matrice (QR code) :

173 : 10101101

122 : 01111010

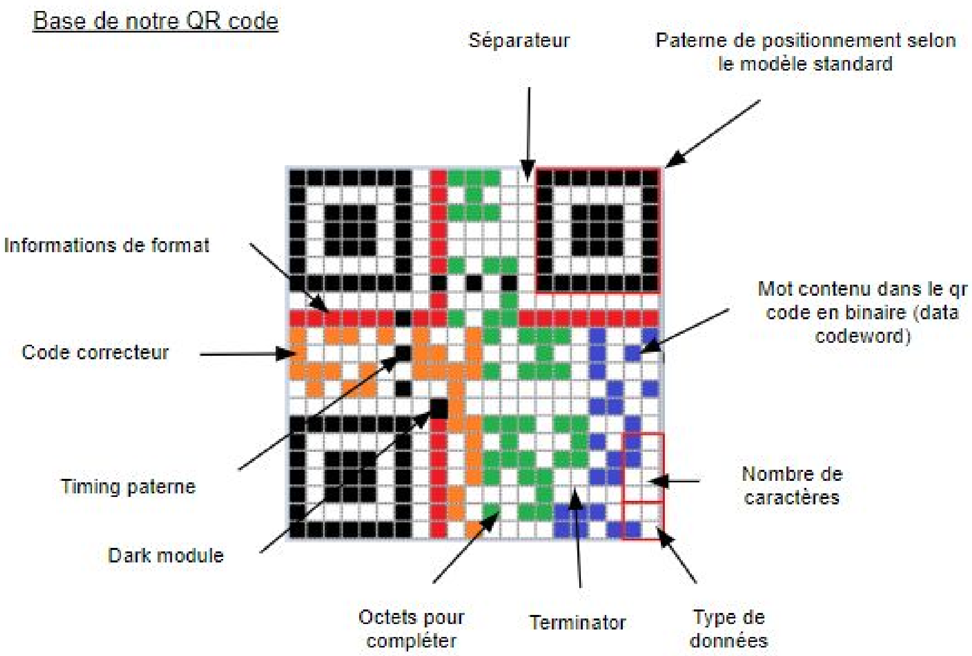
150 : 10010110

61 : 00111101

133 : 10000101

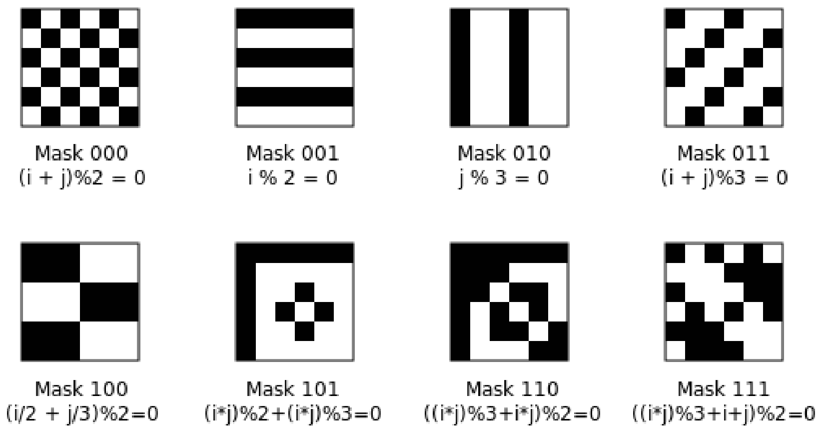
147 : 10010011

94 : 01011110



Pour le dark module, il convient d'expliquer comment on a trouvé son positionnement. Ces coordonnées sont toujours obtenues en effectuant ce calcul : (8, 4*version + 9). Ici, nous sommes en version 1 donc : (8, 4*1 + 9) = (8,13).

Étape 5 : **Générer la matrice et évaluer le résultat qu'elle retourne**



En effectuant les différentes opérations, en prenant i=y et j=x, si la condition est vérifié pour chaque module, alors on met un carré noir. On obtient par conséquent, pour les différents masques, les modèles de figures ci-dessus (nous les avons refait sur le logiciel paint sur 21x21 pixels pour pouvoir les superposer à notre base de QR code (QR coloré ci-avant)).

Masque	Infos de format	QR résultant	Score
000	111011111000100		287
001	111001011110011		428
010	111110110101010		306
011	111100010011101		358
100	110011000101111		394

101	110001100011000		378
110	110110001000001		390
111	110100101110110		348

Tableau recensant les différents QR code en fonction de leur masque

masques	Penality 1	Penality 2	Penality 3	Penality 4	Total
0	176	111	0	0	287
1	197	111	120	0	428
2	176	90	40	0	306
3	180	138	40	0	358
4	179	135	80	0	394
5	191	147	40	0	378
6	178	162	40	10	390
7	185	123	40	0	348

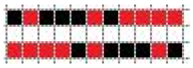
Tableau des scores de pénalités

Ces scores de pénalité sont obtenus selon 4 critères :

- Le premier est décerné en fonction du nombre de pixel de la même couleur d'affilée sur une même ligne ou une même colonne. S'il y en a moins de 5 d'affilée aucune pénalité n'est donnée, s'il y a pile 5 modules de la même couleur d'affilée alors une pénalité de 3 points est décernée. Ensuite, s'il y a plus de 5 modules de la même couleur, on augmente le score de 1 pour chaque pixel (ex: 6

pixels de même couleur sur une même ligne = 4 points de pénalité, 7 = 5 points de pénalité ainsi de suite.)

- Le deuxième est décerné en fonction du nombre de carrée de 2 pixels sur 2 de même couleur, 3 points de pénalité sont alors donnés pour chacun de ces carrés.
- Le troisième est celui qui donne la plus grosse pénalité. En effet, si le pattern suivant est trouvé dans le code, la pénalité est de 40 points par pattern trouvé.



(j'ai représenté les pixels blancs en rouge pour que cela soit plus visuel)

- Le dernier est donné si la différence entre le nombre de carrée blanc et de carrée noir est trop importante, plus la différence est grande plus la prénalité est grande.

Vous devez vous demander comment on a trouvé les informations de format. Et bien, cela est très simple. Pour ne pas effectuer 8 fois les mêmes calculs, nous ne développerons que pour le masque 000 à savoir, comment trouve-t'on 111011111000100 ?

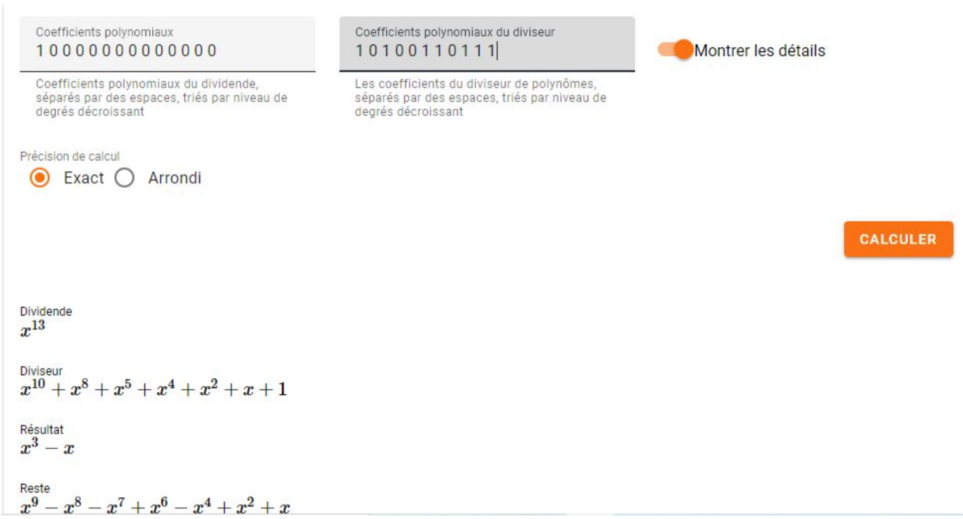
Nous avons utilisé le niveau de correction d'erreur Low (01) et le motif de masque 000, la séquence binaire de cinq bits commence donc par 01000

Maintenant que nous avons les cinq bits pour la chaîne de format, nous devons utiliser cette dernière pour générer les dix bits de correction d'erreur.

A contrario de l'étape 3, utiliser la correction d'erreur en utilisant du Reed-Solomon est un peu plus facile. En effet, dans ce cas, les polynômes contiennent moins de termes et leurs coefficients sont tous des 1 ou 0.

La chaîne de 5 bits est encodée avec le polynôme générateur 10100110111 comme indiqué dans le cours. On souhaite diviser la chaîne de 5 bits contenant le masque et le niveau de correction d'erreur par le polynôme générateur.

Pour se faire on va multiplier 01000 par la puissance du polynôme générateur à savoir 10. Si on retranscrit ces nombres binaires en polynômes, cela nous donne : $X^{13}/(X^{10}+X^8+X^5+X^4+X^2+X+1)$.



ATTENTION Si le polynôme n'est pas de degré 9, il convient de rajouter des 0 à gauche du polynôme pour avoir une chaîne binaire de 10 bits. Le polynôme reste donc identique $X^9+X^8+X^7+X^6+X^4+X^2+X$ = > 1111010110

On accole la chaîne de 5 bits trouvée précédemment, 01000, en la plaçant à gauche de la chaîne binaire, correspondant au polynôme. Ce qui donne :

$X^{13}+X^9+X^8+X^7+X^6+X^4+X^2+X$ => 010001111010110

Nous savons aussi, d'après les spécificités du QR code, qu'il faut XORé (soustraire), le polynôme trouvé précédemment avec le polynôme $X^{14}+X^{12}+X^{10}+X^4+X$:

"the QR code specification says to XOR the result with the following binary string : 101010000010010"

Par conséquent, on a : $X^{13}+X^9+X^8+X^7+X^6+X^4+X^2+X$ - $(X^{14}+X^{12}+X^{10}+X^4+X)$ =

$X^{14}+X^{13}+X^{12}+X^{10}+X^9+X^8+X^7+X^6+X^2$ => 111011111000100

On retrouve donc le polynôme indiqué dans le tableau recensant les différents masques. Nous n'avons donc plus qu'à placer les informations de format à leurs places correspondantes.

ATTENTION Le nombre 0 dans l'image ci-dessous correspond au MSB (Most Significant Bit) et le nombre 14 au LSB (Low Significant Bit).

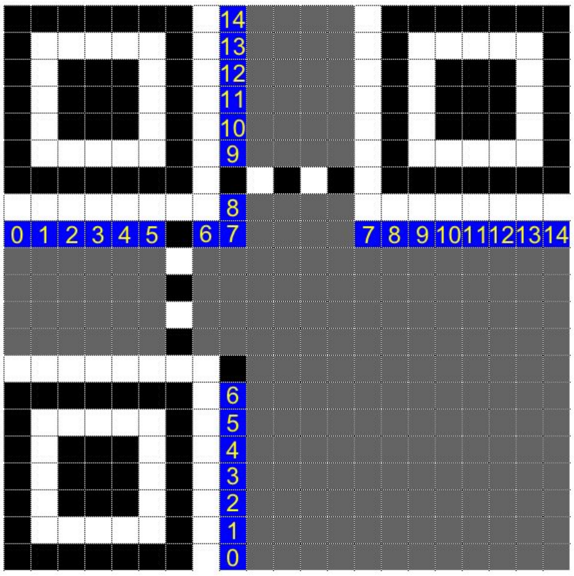


Schéma permettant de placer correctement les data infos

Étape 6 : **Générer le QR code au format image**

QR code final, avec marqué "Hello", en utilisant le masque 000 car c'est celui qui a obtenu le score le plus faible, donc c'est le QR le plus fiable

Contrairement à ce que l'on pourrait penser, il n'existe que très peu de ressources à notre disposition pour réaliser, et comprendre le fonctionnement d'un QR code de a à z. C'est donc pour cela que nous ne citons que très peu de sources en plus des données énoncées dans le polycopié de cours.

Comme vous avez pu le constater nous nous sommes grandement aidé du site thonky.com, où un tutoriel de la création d'un QR code étape par étape est présenté. Ce dernier, tout en anglais, n'est parfois pas facile à comprendre, c'est pour cela que nous nous sommes appropriés le processus et l'avons rédigé par nous même, avec nos propres mots et avec nos propres moyens dans ce rapport (choix personnels (paint, tableur excel, déroulés/compréhension des calculs)…).
Se détacher du tutoriel, nous a permis de développer nos propres capacités, à travers de nouveaux raisonnement, de nouveaux choix de recherches… Nous avons aussi croisé les sources de manière à obtenir quelque chose de fonctionnel nous appartenant. En bref, de gagner en autonomie, de créer un QR code dont on ne connaissait pas du tout le fonctionnement (ou presque) lors du commencement du projet.

Cette méthodologie, en mode projet, est selon nous la plus pédagogue. On apprend à notre rythme, en recherchant, en s'entraidant et bien entendu, en s'investissant. Dans votre mail présentant ce sujet vous nous demander d'estimer la note que l'on pourrait avoir en fonction du travail que l'on a fourni. Compte tenu de notre investissement, du temps (environ 2.5 semaines à hauteur d'environ 1h30 par jour (oui, on s'est planté plusieurs fois sur les calculs qu'il a fallu refaire ;))) que ce projet nous a pris, mais pas seulement. Compte tenu aussi du fait que l'on a compris tout ce que l'on faisait, il serait légitime que l'on ait une bonne note (18,19 ou 20).

Sources :

Type	Lien
Site web pour faire un QRcode	https://www.thonky.com/qr-code-tutorial/data-encoding
Pdf sur les QRcode	http://tpe-codebarre2d.e-monsite.com/pages/page.html#page4
Pdf QRcode	http://remy-manu.no-ip.biz/C++/PDF/QRCode.pdf
antilog/log table jusqu'à 255	https://www.thonky.com/qr-code-tutorial/log-antilog-table