入学年度		学部	学 科		組		番　号			検	フリガナ	
		B		1							氏 名	

学籍番号を実際に QR コードにしてみよう．

- QR コードの型

中大の学籍番号は大文字のみのアルファベットと数字あわせて 11 文字からなるので「英数字モード」を用いることにする．この文字数なら誤り訂正レベルが高めの「レベル Q」を選択しても 1 型（21 × 21 セル）に収まるので，1-Q 型を選ぶことにする．また，マスクパターンは本来出来上がったデータの上に掛けてみて一番良いものを選ぶべきなのだが，ここではそれを省略し，予め市松模様のパターン（000 型）をかけることに決めておく．

型番（バージョン）： 1（21 × 21 セル）
誤り訂正レベル： Q（2 進指示子 11，復元能力 25%）
マスクパターン： 000（市松模様）
データモード： 0010（英数字モード）

- 形式情報

誤り訂正レベルとマスクパターンは「形式情報」としてタイミングパターンのすぐそばに格納される．今の場合，11000 を BCH(15, 5) で符号化し，さらに 101010000010010 というマスクを掛けてつくられる．結果は次のようになる．

011010101011111

- データの bit 列化

さて，次にデータ領域に配置するデータを準備する．まず，最初の 4bit はモードを指示するためのもので，学籍番号では英数字モードを用いるので 0010 とする．次に文字数を指示する必要があるが，英数字モードの場合の最大格納文字数の関係から，これを 9bit で表す．中大の学籍番号は 11 文字なので，これを 2 進法で表示すると 1011 であるが，これに 0 を加えて 9bit 化し 000001011 とする．

そして，いよいよ実際のデータを bit 列になおす．英数字モードではまず下表の通りに各文字を数字化する．なぜ 45 文字が使用可能かというと，$45^2 = 2025 \fallingdotseq 2048 = 2^{11}$ なので，2 文字の組を 11bit で表すことができ，効率よく符号化できるからである．2 文字の組は「45 進法」で表された 2 桁の数であると考え，例えば，‘DX’ という 2 文字の組は，‘D’ ‘X’$_{(45)}$ =‘D’×45+‘X’ とみなす．そして，‘D’，‘X’ を下の表から，それぞれ 13，33 に変換し，‘DX’= $13 \times 45 + 33 = 618$ とする．さらに，これを 11bit の 2 進法で表し，$1001101010_{(2)}$ とする．ここで，$45^2 < 2^{11}$ であることから，この 2 進法で表された数は 11 桁以下になっている．そこで，これの最初に 0 を加え，01001101010 という 11 bit の 0 と 1 の列とする．

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z		$	%	*
20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39

+	-	.	/	:
40	41	42	43	44

いくつかの文字列のデータは，2 文字ずつに区切ってそれらを 11 bit の文字列としていく．文字数が奇数の場合の最後に残った 1 文字は対応する表の値をそのまま 2 進法で表し，6 bit で表記する．

学生証番号	2	5	B								
「10 進法化」	95										
11bit 化	00001011111										

すべてを bit 化したら，最後に終端パターンとして 0000 を付加する．

$$\underbrace{0010}_{\text{英数字モード}}\ \underbrace{000001011}_{\text{文字数 11}}\ \underbrace{00001011111}_{\text{“25”}}\ \underbrace{\cdots}_{\text{“B・”}}\ \cdots\ \underbrace{0000}_{\text{終端パターン}}$$

こうして得られたデータを 8 bit ごと（1 byte ごと）に区切り直す．最後のビット列が 8bit 未満の場合は 0 で埋める．また，1-Q 型では RS(26, 13, 6) 符号を用いるので，得られた byte 数が情報 byte 数である 13 に満たない場合は "11101100" および "00010001" という「埋め草パターン」を交互に付加する．

英数字モード				文字数 11								“25”											
0	0	1	0	0	0	0	0	0	1	0	1	1											

“B・”																							

		終端パターン				0 fill		埋め草パターン 1								埋め草パターン 2							
		0	0	0	0	0	0	1	1	1	0	1	1	0	0	0	0	0	1	0	0	0	1

埋め草パターン 1							
1	1	1	0	1	1	0	0

このようにして，13byte からなる情報語を得る．

	8bit データ							
1.	0	0	1	0	0	0	0	0
2.	0	1	0	1	1	0	0	0
3.								
4.								
5.								
6.								
7.								
8.								
9.								
10.								
11.								
12.								
13.	1	1	1	0	1	1	0	0

担当：鍬田 政人 (kuwata.04f@g.chuo-u.ac.jp)

- 誤り訂正符号化

ここまでで学籍番号から 13 byte（8 bit の組 13 個）の 0 と 1 からなる情報語を作った．次に，これに誤り訂正コード語を加えて符号語をつくる．

1-Q 型の QR コードでは RS 符号（リード・ソロモン符号）と呼ばれる符号化法を用いる．RS 符号は $GF(2^8) = GF(256) = \mathbb{F}_{256}$ という数の体系を用いて作られる．$\mathbb{F}_{256}$ は $GF(2) = \mathbb{F}_2$ に

$$\gamma^8 + \gamma^4 + \gamma^3 + \gamma^2 + 1 = 0$$

をみたす γ という “虚数” を付け加えた数の体系である．$\mathbb{F}_{256}$ の数は γ の 7 次以下の多項式で表され（**加法表示**），8 bit = 1 byte の情報を保持する．また，$\mathbb{F}_{256}$ の 0 以外の数は γ^k $(k = 0, 1, \ldots, 254)$ と表せることも思い出しておく（**乗法表示**）．BCH 符号では，情報を 0 と 1 を係数に持つ多項式，すなわち “1 bit” 係数の多項式で表し，それに剰余などの代数的操作を加えて符号語を作るのであった．これに対し，RS 符号では，係数が “1 byte” である多項式に同様の操作を用いて誤り訂正符号を作る．

ここで用いる RS(26, 13) は 13 byte の情報語に誤り訂正部分を加えて 26 byte としたものを符号語とする符号である．ここまでで作ったデータは 13 byte あるが，まず，その各 byte を γ の 7 次以下の多項式とみなし，$\mathbb{F}_{256}$ の数とみなす．たとえば，1 行目の “00100000” は γ^5，2 行目の “01011000” は $\gamma^6 + \gamma^4 + \gamma^3$ などとする．そして，この 13 byte の情報語から，係数が γ の 7 次以下の式である x の 12 次の多項式をつくる．こうして情報語から

$$q(x) = \gamma^5 x^{12} + (\gamma^6 + \gamma^4 + \gamma^3)x^{11} + \cdots + (\gamma^7 + \gamma^6 + \gamma^5 + \gamma^3 + \gamma^2)$$

という情報多項式で表せる．

1 前回作成した情報語から，情報多項式 $q(x)$ をつくれ．

$$\begin{aligned}
q(x) = (\quad &) x^{12} \\
+(\quad &) x^{11} \\
+(\quad &) x^{10} \\
+(\quad &) x^{9} \\
+(\quad &) x^{8} \\
+(\quad &) x^{7} \\
+(\quad &) x^{6} \\
+(\quad &) x^{5} \\
+(\quad &) x^{4} \\
+(\quad &) x^{3} \\
+(\quad &) x^{2} \\
+(\quad &) x \\
+(\quad &)
\end{aligned}$$

BCH 符号では，情報多項式 $q(x)$ から生成多項式 $g(x)$ を用いて送信多項式を作るのであった．RS 符号でも，BCH 符号と同じ要領で送信多項式を作る．RS(26, 13) では，生成多項式 $g(x)$ を

$$g(x) = (x - 1)(x - \gamma)(x - \gamma^2)(x - \gamma^3) \times \cdots \times (x - \gamma^{12})$$

として，送信多項式 $u(x)$ を $g(x)$ 用いて次のようにする．

$$u(x) = q(x)x^{13} + \big(q(x)x^{13} \text{ を } g(x) \text{ で割った余り}\big)$$

このように定義することにより，送信多項式は $u(x)$ は生成多項式 $g(x)$ で割り切れることがわかる．（正確には $u(x)$ を $g(x)$ を割った余りは $q(x)$ を $g(x)$ を割った余りの 2 倍であるが，$\mathbb{F}_{256}$ では $2 = 1 + 1 = 0$ が成り立つので，余りが 0 になる．）

このような $u(x)$ を手計算で求めるのはかなり複雑なので，ここでは，Mathematica ファイルをダウンロードし，それを用いて計算する．そうして，得られた送信語を下の表に写す．

1.	0	0	1	0	0	0	0	0
2.	0	1	0	1	1	0	0	0
3.								
4.								
5.								
6.								
7.								
8.								
9.								
10.								
11.								
12.								
13.	1	1	1	0	1	1	0	0

14.								
15.								
16.								
17.								
18.								
19.								
20.								
21.								
22.								
23.								
24.								
25.								
26.								

次回は，このデータにマスク処理と呼ばれる処理を施し，形式情報を加えて，所定の位置に黒（1）と白（0）を配置して QR コードを作成する．

担当：鍬田 政人 (kuwata.04f@g.chuo-u.ac.jp)