Generalized Reed-Solomon Codes

John McCall

Division of Science and Mathematics
University of Minnesota, Morris
Morris, Minnesota, USA

April 15, 2014

Overview

- Data transmission has become vital in today's society.
- Transmission methods are not perfect.
- Error correcting codes help to alleviate the burden of transmission.

Outline

1. Defining the Playing Field
2. Codes
3. Generalized Reed-Solomon Codes
4. Conclusion

Outline

1. Defining the Playing Field
2. Codes
3. Generalized Reed-Solomon Codes
4. Conclusion

Introducing $\mathbb{F}_{64}$

The 64 symbols chosen to be our elements.

Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
32	20	040		Space	64	40	100	@	@
33	21	041	!	!	65	41	101	A	A
34	22	042	"	"	66	42	102	B	B
35	23	043	#	#	67	43	103	C	C
36	24	044	$	$	68	44	104	D	D
37	25	045	%	%	69	45	105	E	E
38	26	046	&	&	70	46	106	F	F
39	27	047	'	'	71	47	107	G	G
40	28	050	(	(	72	48	110	H	H
41	29	051	)	)	73	49	111	I	I
42	2A	052	*	*	74	4A	112	J	J
43	2B	053	+	+	75	4B	113	K	K
44	2C	054	,	,	76	4C	114	L	L
45	2D	055	-	-	77	4D	115	M	M
46	2E	056	.	.	78	4E	116	N	N
47	2F	057	/	/	79	4F	117	O	O
48	30	060	0	0	80	50	120	P	P
49	31	061	1	1	81	51	121	Q	Q
50	32	062	2	2	82	52	122	R	R
51	33	063	3	3	83	53	123	S	S
52	34	064	4	4	84	54	124	T	T
53	35	065	5	5	85	55	125	U	U
54	36	066	6	6	86	56	126	V	V
55	37	067	7	7	87	57	127	W	W
56	38	070	8	8	88	58	130	X	X
57	39	071	9	9	89	59	131	Y	Y
58	3A	072	:	:	90	5A	132	Z	Z
59	3B	073	;	;	91	5B	133	[	[
60	3C	074	<	<	92	5C	134	\	\
61	3D	075	=	=	93	5D	135	]	]
62	3E	076	>	>	94	5E	136	^	^
63	3F	077	?	?	95	5F	137	_	_

Figure : Our Elements. Taken from: `http://www.asciitable.com/`

Addition in $\mathbb{F}_{64}$

$\boxed{!} + \boxed{} = \boxed{!}$

$\boxed{!} + \boxed{!} = \boxed{}$

$\boxed{!} + \boxed{"} = \boxed{\#}$

$\boxed{1} + \boxed{2} = \boxed{\#}$

		!	"	#	$	%	&	'	(	)	*	+	,	-	.	/	0	1	2
		!	"	#	$	%	&	'	(	)	*	+	,	-	.	/	0	1	2
!	!		#	"	%	$	'	&	)	(	+	*	-	,	/	.	1	0	3
"	"	#		!	&	'	$	%	*	+	(	)	.	/	,	-	2	3	0
#	#	"	!		'	&	%	$	+	*	)	(	/	.	-	,	3	2	1
$	$	%	&	'		!	"	#	,	-	.	/	(	)	*	+	4	5	6
%	%	$	'	&	!		#	"	-	,	/	.	)	(	+	*	5	4	7
&	&	'	$	%	"	#		!	.	/	,	-	*	+	(	)	6	7	4
'	'	&	%	$	#	"	!		/	.	-	,	+	*	)	(	7	6	5
(	(	)	*	+	,	-	.	/		!	"	#	$	%	&	'	8	9	:
)	)	(	+	*	-	,	/	.	!		#	"	%	$	'	&	9	8	;
*	*	+	(	)	.	/	,	-	"	#		!	&	'	$	%	:	;	8
+	+	*	)	(	/	.	-	,	#	"	!		'	&	%	$	;	:	9
,	,	-	.	/	(	)	*	+	$	%	&	'		!	"	#	<	=	>
-	-	,	/	.	)	(	+	*	%	$	'	&	!		#	"	=	<	?
.	.	/	,	-	*	+	(	)	&	'	$	%	"	#		!	>	?	<
/	/	.	-	,	+	*	)	(	'	&	%	$	#	"	!		?	>	=
0	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?		!	"
1	1	0	3	2	5	4	7	6	9	8	;	:	=	<	?	>	!		#
2	2	3	0	1	6	7	4	5	:	;	8	9	>	?	<	=	"	#	

Figure : A section of the addition table for $\mathbb{F}_{64}$.

Multiplication in $\mathbb{F}_{64}$

$\boxed{!} * \boxed{} = \boxed{}$

$\boxed{!} * \boxed{\#} = \boxed{\#}$

$\boxed{\&} * \boxed{?} = \boxed{!}$

$\boxed{3} * \boxed{\mathtt{A}} = \boxed{\mathtt{H}}$

	!	"	#	$	%	&	'	(	)	*	+	,	-	.	/	0	1	2
!	!	"	#	$	%	&	'	(	)	*	+	,	-	.	/	0	1	2
"	"	$	&	(	*	,	.	0	2	4	6	8	:	<	>	@	B	D
#	#	&	%	,	/	*	)	8	;	>	=	4	7	2	1	P	S	V
$	$	(	,	0	4	8	<	@	D	H	L	P	T	X	\	#	'	+
%	%	*	/	4	1	>	;	H	M	B	G	\	Y	V	S	3	6	9
&	&	,	*	8	>	4	2	P	V	\	Z	H	N	D	B	C	E	O
'	'	.	)	<	;	2	5	X	_	V	Q	D	C	J	M	S	T	]
(	(	0	8	@	H	P	X	#	+	3	;	C	K	S	[	&	.	6
)	)	2	;	D	M	V	_	+	"	9	0	O	F	]	T	6	?	$
*	*	4	>	H	B	\	V	3	9	'	-	[	Q	O	E	F	L	R
+	+	6	=	L	G	Z	Q	;	0	-	&	W	\	A	J	V	]	@
,	,	8	4	P	\	H	D	C	O	[	W	3	?	+	'	%	)	=
-	-	:	7	T	Y	N	C	K	F	Q	\	?	2	%	(	5	8	/
.	.	<	2	X	V	D	J	S	]	O	A	+	%	7	9	E	K	Y
/	/	>	1	\	S	B	M	[	T	E	J	'	(	9	6	U	Z	K
0	0	@	P	#	3	C	S	&	6	F	V	%	5	E	U	,	<	L
1	1	B	S	'	6	E	T	.	?	L	]	)	8	K	Z	<	-	^
2	2	D	V	+	9	O	]	6	$	R	@	=	/	Y	K	L	^	(

Figure : A section of the multiplication table for $\mathbb{F}_{64}$.

Multiplication in $\mathbb{F}_{64}$

		!	"	#	$	%	&	'	(	)	*	+	,	-	.	/	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
!		!	"	#	$	%	&	'	(	)	*	+	,	-	.	/	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
"		"	$	&	(	*	,	.	0	2	4	6	8	:	<	>	@	B	D	F	H	J	L	N	P	R	T	V	X	Z	\	^	#	!	'	%	+	)	/	-	3	1	7	5	;	9	?	=	C	A	G	E	K	I	O	M	S	Q	W	U	[	Y	_	]
#		#	&	%	,	/	*	)	8	;	>	=	4	7	2	1	P	S	V	U	\	_	Z	Y	H	K	N	M	D	G	B	A	C	@	E	F	O	L	I	J	[	X	]	^	W	T	Q	R	3	0	5	6	?	<	9	:	+	(	-	.	'	$	!	"
$		$	(	,	0	4	8	<	@	D	H	L	P	T	X	\	#	'	+	/	3	7	;	?	C	G	K	O	S	W	[	_	&	"	.	*	6	2	>	:	F	B	N	J	V	R	^	Z	%	!	-	)	5	1	=	9	E	A	M	I	U	Q	]	Y
%		%	*	/	4	1	>	;	H	M	B	G	\	Y	V	S	3	6	9	<	'	"	-	(	[	^	Q	T	O	J	E	@	F	C	L	I	R	W	X	]	.	+	$	!	:	?	0	5	U	P	_	Z	A	D	K	N	=	8	7	2	)	,	#	&
&		&	,	*	8	>	4	2	P	V	\	Z	H	N	D	B	C	E	O	I	[	]	W	Q	3	5	?	9	+	-	'	!	%	#	)	/	=	;	1	7	U	S	Y	_	M	K	A	G	F	@	J	L	^	X	R	T	6	0	:	<	.	(	"	$
'		'	.	)	<	;	2	5	X	_	V	Q	D	C	J	M	S	T	]	Z	O	H	A	F	+	,	%	"	7	0	9	>	E	B	K	L	Y	^	W	P	=	:	3	4	!	&	/	(	6	1	8	?	*	-	$	#	N	I	@	G	R	U	\	[
(		(	0	8	@	H	P	X	#	+	3	;	C	K	S	[	&	.	6	>	F	N	V	^	%	-	5	=	E	M	U	]	,	$	<	4	L	D	\	T	/	'	?	7	O	G	_	W	*	"	:	2	J	B	Z	R	)	!	9	1	I	A	Y	Q
)		)	2	;	D	M	V	_	+	"	9	0	O	F	]	T	6	?	$	-	R	[	@	I	=	4	/	&	Y	P	K	B	L	E	^	W	(	!	:	3	G	N	U	\	#	*	1	8	Z	S	H	A	>	7	,	%	Q	X	C	J	5	<	'	.
*		*	4	>	H	B	\	V	3	9	'	-	[	Q	O	E	F	L	R	X	.	$	:	0	U	_	A	K	=	7	)	#	/	%	;	1	G	M	S	Y	<	6	(	"	T	^	@	J	I	C	]	W	!	+	5	?	Z	P	N	D	2	8	&	,
+		+	6	=	L	G	Z	Q	;	0	-	&	W	\	A	J	V	]	@	K	:	1	,	'	M	F	[	P	!	*	7	<	O	D	Y	R	#	(	5	>	T	_	B	I	8	3	.	%	9	2	/	$	U	^	C	H	"	)	4	?	N	E	X	S
,		,	8	4	P	\	H	D	C	O	[	W	3	?	+	'	%	)	=	1	U	Y	M	A	F	J	^	R	6	:	.	"	*	&	2	>	Z	V	B	N	I	E	Q	]	9	5	!	-	/	#	7	;	_	S	G	K	L	@	T	X	<	0	$	(
-		-	:	7	T	Y	N	C	K	F	Q	\	?	2	%	(	5	8	/	"	A	L	[	V	^	S	D	I	*	'	0	=	J	G	P	]	>	3	$	)	!	,	;	6	U	X	O	B	_	R	E	H	+	&	1	<	4	9	.	#	@	M	Z	W
.		.	<	2	X	V	D	J	S	]	O	A	+	%	7	9	E	K	Y	W	=	3	!	/	6	8	*	$	N	@	R	\	)	'	5	;	Q	_	M	C	Z	T	F	H	"	,	>	0	L	B	P	^	4	:	(	&	?	1	#	-	G	I	[	U
/		/	>	1	\	S	B	M	[	T	E	J	'	(	9	6	U	Z	K	D	)	&	7	8	.	!	0	?	R	]	L	C	I	F	W	X	5	:	+	$	2	=	,	#	N	A	P	_	<	3	"	-	@	O	^	Q	G	H	Y	V	;	4	%	*
0		0	@	P	#	3	C	S	&	6	F	V	%	5	E	U	,	<	L	\	/	?	O	_	*	:	J	Z	)	9	I	Y	8	(	X	H	;	+	[	K	>	.	^	N	=	-	]	M	4	$	T	D	7	'	W	G	2	"	R	B	1	!	Q	A
1		1	B	S	'	6	E	T	.	?	L	]	)	8	K	Z	<	-	^	0	;	*	Y	H	2	#	P	A	5	$	W	F	X	I	:	+	_	N	=	,	V	G	4	%	Q	@	3	"	D	U	&	7	C	R	!	O	J	[	(	9	M	\	/	>
2		2	D	V	+	9	O	]	6	$	R	@	=	/	Y	K	L	^	(	:	G	U	#	1	Z	H	>	,	Q	C	5	'	;	)	_	M	0	"	T	F	-	?	I	[	&	4	B	P	W	E	3	!	\	N	8	*	A	S	%	7	J	X	.	<
3		3	F	U	/	<	I	Z	>	-	X	K	1	"	W	D	\	0	:	)	S	@	5	&	B	Q	$	7	M	^	+	8	[	H	=	.	T	G	2	!	E	V	#	O	J	Y	,	?	'	4	A	R	(	;	N	]	9	*	_	L	6	%	P	C
4		4	H	\	3	'	[	O	F	R	.	:	U	A	=	)	/	;	G	S	<	(	T	@	I	]	!	5	Z	N	2	&	>	*	V	B	-	9	E	Q	X	L	0	$	K	_	#	7	1	%	Y	M	"	6	J	^	W	C	?	+	D	P	,	8
5		5	J	_	7	"	]	H	N	[	$	1	Y	L	3	&	?	*	U	@	(	=	B	W	Q	D	;	.	F	S	,	9	^	K	4	!	I	\	#	6	0	%	Z	O	'	2	M	X	A	T	+	>	V	C	<	)	/	:	E	P	8	-	R	G
6		6	L	Z	;	-	W	A	V	@	:	,	M	[	!	7	O	Y	#	5	T	B	8	.	9	/	U	C	"	4	N	X	=	+	Q	G	&	0	J	\	K	]	'	1	P	F	<	*	R	D	>	(	I	_	%	3	$	2	H	^	?	)	S	E
7		7	N	Y	?	(	Q	F	^	I	0	'	A	V	/	8	_	H	1	&	@	W	.	9	!	6	O	X	>	)	P	G	]	J	3	$	B	U	,	;	#	4	M	Z	<	+	R	E	"	5	L	[	=	*	S	D	\	K	2	%	C	T	-	:
8		8	P	H	C	[	3	+	%	=	U	M	F	^	6	.	*	2	Z	B	I	Q	9	!	/	7	_	G	L	T	<	$	4	,	D	\	W	O	'	?	1	)	A	Y	R	J	"	:	>	&	N	V	]	E	-	5	;	#	K	S	X	@	(	0
9		9	R	K	G	^	5	,	-	4	_	F	J	S	8	!	:	#	H	Q	]	D	/	6	7	.	E	\	P	I	"	;	T	M	&	?	3	*	A	X	Y	@	+	2	>	'	L	U	N	W	<	%	)	0	[	B	C	Z	1	(	$	=	V	O
:		:	T	N	K	Q	?	%	5	/	A	[	^	D	*	0	J	P	>	$	!	;	U	O	_	E	+	1	4	.	@	Z	7	-	C	Y	\	F	(	2	"	8	V	L	I	S	=	'	]	G	)	3	6	,	B	X	H	R	<	&	#	9	W	M
;		;	V	M	O	T	9	"	=	&	K	P	R	I	$	?	Z	A	,	7	5	.	C	X	G	\	1	*	(	3	^	E	W	L	!	:	8	#	N	U	J	Q	<	'	%	>	S	H	-	6	[	@	B	Y	4	/	0	+	F	]	_	D	)	2
<		<	X	D	S	0	+	7	E	Y	=	!	6	*	N	R	)	5	Q	M	Z	F	"	>	L	P	4	(	?	#	G	[	2	.	J	V	A	]	9	%	W	K	/	3	$	8	\	@	;	'	C	_	H	T	O	,	^	B	&	:	-	1	U	I
=		=	Z	G	W	J	-	0	M	P	7	*	:	'	@	]	9	$	C	^	N	S	4	)	T	I	.	3	#	>	Y	D	R	O	(	5	%	8	_	B	?	"	E	X	H	U	2	/	K	V	1	,	<	!	F	[	&	;	\	A	Q	L	+	6
>		>	\	B	[	E	'	9	U	K	)	7	.	0	R	L	I	W	5	+	2	,	N	P	<	"	@	^	G	Y	;	%	1	/	M	S	J	T	6	(	D	Z	8	&	?	!	C	]	X	F	$	:	#	=	_	A	-	3	Q	O	V	H	*	4
?		?	^	A	_	@	!	>	]	B	#	<	"	=	\	C	Y	F	'	8	&	9	X	G	$	;	Z	E	[	D	%	:	Q	N	/	0	.	1	P	O	,	3	R	M	S	L	-	2	(	7	V	I	W	H	)	6	U	J	+	4	*	5	T	K
@		@	#	C	&	F	%	E	,	L	/	O	*	J	)	I	8	X	;	[	>	^	=	]	4	T	7	W	2	R	1	Q	P	0	S	3	V	6	U	5	\	<	_	?	Z	:	Y	9	H	(	K	+	N	.	M	-	D	$	G	'	B	"	A	!
A		A	!	@	"	C	#	B	$	E	%	D	&	G	'	F	(	I	)	H	*	K	+	J	,	M	-	L	.	O	/	N	0	Q	1	P	2	S	3	R	4	U	5	T	6	W	7	V	8	Y	9	X	:	[	;	Z	<	]	=	\	>	_	?	^
B		B	'	E	.	L	)	K	<	^	;	Y	2	P	5	W	X	:	_	=	V	4	Q	3	D	&	C	!	J	(	M	/	S	1	T	6	]	?	Z	8	O	-	H	*	A	#	F	$	+	I	,	N	%	G	"	@	7	U	0	R	9	[	>	\
C		C	%	F	*	I	/	L	4	W	1	R	>	]	;	X	H	+	M	.	B	!	G	$	\	?	Y	:	V	5	S	0	3	P	6	U	9	Z	<	_	'	D	"	A	-	N	(	K	[	8	^	=	Q	2	T	7	O	,	J	)	E	&	@	#
D		D	+	O	6	R	=	Y	L	(	G	#	Z	>	Q	5	;	_	0	T	-	I	&	B	W	3	\	8	A	%	J	.	V	2	]	9	@	$	K	/	:	^	1	U	,	H	'	C	M	)	F	"	[	?	P	4	!	E	*	N	7	S	<	X
E		E	)	L	2	W	;	^	D	!	M	(	V	3	_	:	+	N	"	G	9	\	0	U	O	*	F	#	]	8	T	1	6	S	?	Z	$	A	-	H	R	7	[	>	@	%	I	,	=	X	4	Q	/	J	&	C	Y	<	P	5	K	.	B	'
F		F	/	I	>	X	1	W	\	:	S	5	B	$	M	+	[	=	T	2	E	#	J	,	'	A	(	N	9	_	6	P	U	3	Z	<	K	-	D	"	)	0	&	@	7	Q	8	^	.	H	!	G	O	V	?	Y	R	4	]	;	L	*	C	%
G		G	-	J	:	]	7	P	T	3	Y	>	N	)	C	$	K	,	F	!	Q	6	\	;	?	X	2	U	%	B	(	0	5	R	8	_	/	H	"	E	A	&	L	+	[	<	V	1	^	9	S	4	D	#	I	.	*	M	'	@	O	W	=	Z
H		H	3	[	F	.	U	=	/	G	<	T	I	!	Z	2	>	V	-	E	X	0	K	#	1	Y	"	J	W	?	D	,	\	4	O	'	:	R	)	A	S	;	@	(	5	]	&	N	B	*	Q	9	$	L	7	_	M	%	^	6	+	C	8	P
I		I	1	X	B	+	S	:	'	N	6	_	E	,	T	=	.	G	?	V	L	%	]	4	)	@	8	Q	K	"	Z	3	<	U	-	D	^	7	0	&	;	R	*	C	Y	O	H	!	2	[	#	J	P	9	A	(	5	\	$	M	W	>	F	/
J		J	7	]	N	$	Y	3	?	U	(	B	Q	;	F	,	^	4	I	#	0	Z	'	M	A	+	V	<	/	E	8	R	_	5	H	"	1	[	&	L	@	*	W	=	.	D	9	S	!	K	6	\	O	%	X	2	>	T	)	C	P	:	G	-
K		K	5	^	J	!	_	4	7	\	"	I	]	6	H	#	N	%	[	0	$	O	1	Z	Y	2	L	'	3	X	&	M	?	T	*	A	U	>	@	+	(	C	=	V	B	)	W	<	Q	:	D	/	;	P	.	E	F	-	S	8	,	G	9	R
L		L	;	W	V	:	M	!	O	#	T	8	9	U	"	N	=	Q	&	J	K	'	P	<	R	>	I	%	$	H	?	S	Z	6	A	-	,	@	7	[	5	Y	.	B	C	/	X	4	G	+	\	0	1	]	*	F	(	D	3	_	^	2	E	)
M		M	9	T	R	?	K	&	G	*	^	3	5	X	,	A	-	@	4	Y	_	2	F	+	J	'	S	>	8	U	!	L	:	W	#	N	H	%	Q	<	]	0	D	)	/	B	6	[	7	Z	.	C	E	(	\	1	P	=	I	$	"	O	;	V
N		N	?	Q	^	0	A	/	_	1	@	.	!	O	>	P	]	3	B	,	#	M	<	R	"	L	=	S	\	2	C	-	Y	7	F	(	'	I	8	V	&	H	9	W	X	6	G	)	$	J	;	U	Z	4	E	+	[	5	D	*	%	K	:	T
O		O	=	R	Z	5	G	(	W	8	J	%	-	B	0	_	M	"	P	?	7	X	*	E	:	U	'	H	@	/	]	2	9	V	$	K	C	,	^	1	N	!	S	<	4	[	)	F	T	;	I	&	.	A	3	\	#	L	>	Q	Y	6	D	+
P		P	C	3	%	U	F	6	*	Z	I	9	/	_	L	<	4	D	W	'	1	A	R	"	>	N	]	-	;	K	X	(	H	8	+	[	M	=	.	^	B	2	!	Q	G	7	$	T	\	,	?	O	Y	)	:	J	V	&	5	E	S	#	0	@
Q		Q	A	0	!	P	@	1	"	S	C	2	#	R	B	3	$	U	E	4	%	T	D	5	&	W	G	6	'	V	F	7	(	Y	I	8	)	X	H	9	*	[	K	:	+	Z	J	;	,	]	M	<	-	\	L	=	.	_	O	>	/	^	N	?
R		R	G	5	-	_	J	8	:	H	]	/	7	E	P	"	T	&	3	A	Y	+	>	L	N	<	)	[	C	1	$	V	K	9	,	^	F	4	!	S	Q	#	6	D	\	.	;	I	?	M	X	*	2	@	U	'	%	W	B	O	(	Z	0	=
S		S	E	6	)	Z	L	?	2	A	W	$	;	H	^	-	D	7	!	R	M	>	(	[	V	%	3	@	_	,	:	I	+	X	N	=	"	Q	G	4	9	J	\	/	0	C	U	&	O	<	*	Y	F	5	#	P	]	.	8	K	T	'	1	B
T		T	K	?	5	A	^	*	J	>	!	U	_	+	4	@	7	C	\	(	"	V	I	=	]	)	6	B	H	<	#	W	N	:	%	Q	[	/	0	D	$	P	O	;	1	E	Z	.	Y	-	2	F	L	8	'	S	3	G	X	,	&	R	M	9
U		U	I	<	1	D	X	-	B	7	+	^	S	&	:	0	'	R	N	;	6	C	_	*	E	O	,	Y	T	!	=	H	.	[	G	2	?	J	V	#	L	9	%	P	]	(	4	A	)	\	@	5	8	M	Q	$	K	>	"	W	Z	/	3	F
V		V	O	9	=	K	R	$	Z	,	5	C	G	1	(	^	W	!	8	N	J	<	%	S	-	[	B	4	0	F	_	)	M	;	"	T	P	&	?	I	7	A	X	.	*	\	E	3	:	L	U	#	'	Q	H	>	@	6	/	Y	]	+	2	D
W		W	M	:	9	N	T	#	R	%	?	H	K	<	&	Q	G	O	*	]	^	)	3	D	5	B	X	/	,	[	A	6	-	Z	@	7	4	C	Y	.	_	(	2	E	F	1	+	\	J	=	'	P	S	$	>	I	8	0	U	"	!	V	L	;
X		X	S	+	E	=	6	N	)	Q	Z	"	L	4	?	G	2	J	A	9	W	/	$	\	;	C	H	0	^	&	-	U	D	<	7	O	!	Y	R	*	M	5	>	F	(	P	[	#	V	.	%	]	3	K	@	8	_	'	,	T	:	B	I	1
Y		Y	Q	(	A	8	0	I	!	X	P	)	@	9	1	H	"	[	S	*	C	:	2	K	#	Z	R	+	B	;	3	J	$	]	U	,	E	<	4	M	%	\	T	-	D	=	5	L	&	_	W	.	G	>	6	O	'	^	V	/	F	?	7	N
Z		Z	W	-	M	7	:	@	9	C	N	4	T	.	#	Y	R	(	%	_	?	E	H	2	K	1	<	F	&	\	Q	+	G	=	0	J	*	P	]	'	^	$	)	S	3	I	D	>	5	O	B	8	X	"	/	U	,	V	[	!	A	;	6	L
[		[	U	.	I	2	<	G	1	J	D	?	X	#	-	V	B	9	7	L	+	P	^	%	S	(	&	]	:	A	O	4	'	\	R	)	N	5	;	@	6	M	C	8	_	$	*	Q	E	>	0	K	,	W	Y	"	T	/	!	Z	=	F	H	3
\		\	[	'	U	)	.	R	I	5	2	N	<	@	G	;	1	M	J	6	D	8	?	C	X	$	#	_	-	Q	V	*	B	>	9	E	7	K	L	O	+	W	P	,	^	"	%	Y	S	/	(	T	&	Z	]	!	:	F	A	=	0	3	4	H
]		]	Y	$	Q	,	(	U	A	<	8	E	0	M	I	4	!	\	X	%	P	-	)	T	@	=	9	D	1	L	H	5	"	_	[	&	S	.	*	W	C	>	:	G	2	O	K	6	#	^	Z	'	R	/	+	V	B	?	;	F	3	N	J	7
^		^	_	!	]	#	"	\	Y	'	&	X	$	Z	[	%	Q	/	.	P	,	R	S	-	(	V	W	)	U	+	*	T	A	?	>	@	<	B	C	=	8	F	G	9	E	;	:	D	0	N	O	1	M	3	2	L	I	7	6	H	4	J	K	5
_		_	]	"	Y	&	$	[	Q	.	,	S	(	W	U	*	A	>	<	C	8	G	E	:	0	O	M	2	I	6	4	K	!	^	\	#	X	'	%	Z	P	/	-	R	)	V	T	+	@	?	=	B	9	F	D	;	1	N	L	3	H	7	5	J

Figure : The complete multiplication table for $\mathbb{F}_{64}$.

Multiplication in $\mathbb{F}_{64}$

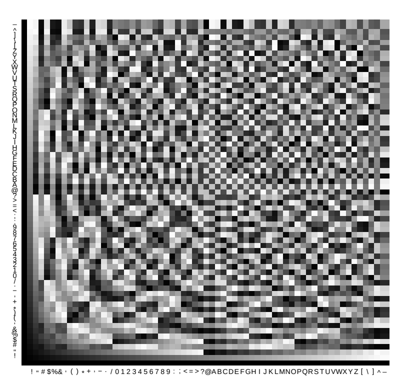

Figure : A greyscale multiplication table for $\mathbb{F}_{64}$.

Polynomials over $\mathbb{F}_{64}$

Notation:

- $\mathbb{Q}[x]$ signifies all polynomials with coefficients in $\mathbb{Q}$.
- $\mathbb{R}[x]$ signifies all polynomials with coefficients in $\mathbb{R}$.

Similarly, we write $\mathbb{F}_{64}[x]$ to denote all polynomials with coefficients in $\mathbb{F}_{64}$.

$\mathbb{F}_{64}[x]_k$ is polynomials of degree less than k

Polynomial Multiplication

$$(\boxed{!}x + \boxed{\#})(\boxed{!}x^2 + \boxed{"}x + \boxed{\%})$$
$$= \boxed{!}x^3 + \boxed{"}x^2 + \boxed{\#}x^2 + \boxed{\%}x + (\boxed{\#} * \boxed{"})x + (\boxed{\#} * \boxed{\%})$$
$$= \boxed{!}x^3 + \boxed{"}x^2 + \boxed{\#}x^2 + \boxed{\%}x + \boxed{\&}x + \boxed{/}$$
$$= \boxed{!}x^3 + \boxed{!}x^2 + \boxed{\#}x + \boxed{/}$$

Recall: $\boxed{!}$ is our multiplicative identity.

Substitution

$$f(x) = \boxed{\texttt{!}}\,x^3 + \boxed{\texttt{!}}\,x^2 + \boxed{\texttt{\#}}\,x + \boxed{\texttt{/}}$$

$$f(\boxed{\texttt{A}}) = (\boxed{\texttt{!}} * \boxed{\texttt{A}}^3) + (\boxed{\texttt{!}} * \boxed{\texttt{A}}^2) + (\boxed{\texttt{\#}} * \boxed{\texttt{A}}) + \boxed{\texttt{/}}$$

$$f(\boxed{\texttt{A}}) = (\boxed{\texttt{!}} * \boxed{\texttt{Q}}) + \boxed{\texttt{!}} + (\boxed{\texttt{\#}} * \boxed{\texttt{Y}}) + \boxed{\texttt{/}}$$

$$f(\boxed{\texttt{A}}) = \boxed{\texttt{Q}} + \boxed{\texttt{Y}} + \boxed{\texttt{@}} + \boxed{\texttt{/}}$$

$$f(\boxed{\texttt{A}}) = \boxed{\texttt{G}}$$

Derivative

$$f(x) = \boxed{!}\,x^3 + \boxed{!}\,x^2 + \boxed{\#}\,x + \boxed{/}$$
$$f'(x) = 3 * \boxed{!}\,x^2 + 2 * \boxed{!}\,x + \boxed{\#}$$

Outline

1. Defining the Playing Field
2. Codes
   - Cyclic Redundancy Check
3. Generalized Reed-Solomon Codes
4. Conclusion

Introduction to Codes

A *code* is a rule for converting information from one representation into another.

- $A \to 1$
- $B \to 2$
- $\vdots$
- $Z \to 26$

Encoding

Encoding is the act of conversion, following the rules of the code.

- HELLO $\rightarrow$ 8 5 12 12 15
- HELLO $\rightarrow$ `H` `E` `L` `L` `O`

Errors

Random errors are a type of error that corrupts individual symbols during transmission.

- H E L L O $\rightarrow$ J E L L O

Burst errors are errors that corrupt a series of contiguous symbols.

- H E L L O $\rightarrow$ H # F ! O

Error Correction

Error detecting codes are a type of code that can detect when these errors occur.
Error correcting codes are a type of code that can correct these errors.

Introduction to CRC

- Used to detect accidental changes in data. It cannot correct these errors.
- Appends a check value to the message prior to transmission.
- After transmission the check value is recomputed and compared to the original value.

Application and Integrity

- CRC is good at detecting random errors and burst errors.
- It is not suitable for detecting intentional modifications to the data.

Example

To compute a binary CRC with a 3-bit check value:

- Start with our message encoded in binary: 1100101
- Make use of a special binary string: 1011

Example

```
 1100101 000
 1011
 0111101 000
  1011
 0010001 000
   1011
 0000111 000
     101 1
 0000010 100
      10 11
-------------
 0000000 010
```

Example

```
1100101 010
1011
0111101 010
 1011
0010001 010
  1011
0000111 010
    101 1
0000010 110
     10 11
-------------
0000000 000
```

Example

If an error occurs:

```
 1010101 010
 1011
 0001101 010
    1011
 0000110 010
     101 1
 0000011 110
      10 11
 0000001 000
       1 011
-------------
 0000000 011
```

Since $011 \neq 010$ we have detected that an error occured.

Outline

1 Defining the Playing Field

2 Codes

3 Generalized Reed-Solomon Codes
- Reed-Solomon Codes
- Generalized Reed-Solomon Codes
- Encoding GRS Codes
- Decoding GRS Codes

4 Conclusion

History

- Introduced in 1960 by I.S. Reed and G. Solomon in [2].
- Useful in practical applications and mathematically interesting.
- Used CD players and deep-space communications.

The Code

Sklar, outlines in [3] Reed-Solomon Codes

- Reed-Solomon (RS) codes are a type of error correcting code.
- A RS-code is capable of correcting $\frac{n-k}{2}$ symbol errors.
    - k is the number of data symbols
    - n is the total number of symbols
- Great at correcting burst errors.

Representation

A message encoded using an RS-code is a polynomial with the message symbols embedded in the coefficients. This is called the *message polynomial*.

For our example, the message polynomial would be in in $\mathbb{F}_{64}[x]$.

- $\boxed{\texttt{H}} + \boxed{\texttt{E}}\,x + \boxed{\texttt{L}}\,x^2 + \boxed{\texttt{L}}\,x^3 + \boxed{\texttt{O}}\,x^4$

Generalized Reed-Solomon Codes

- There is an alternate representation, known as Generalized Reed-Solomon (GRS) Codes.
- In this representation the message polynomial is evaluated at n distinct points and each is individually scaled.
- The result is a n-dimensional vector, which is used as the codeword.
- This is the representation that will be used for the remainder of the presentation.

The Code

Let F be a field. Choose nonzero elements $\hat{v} = v_1, v_2..., v_n \in F$ and distinct elements $\hat{\alpha} = \alpha_1, \alpha_2..., \alpha_n \in F$.

$$\text{GRS}_{n,k}(\hat{\alpha}, \hat{v}) = \{(v_1 f(\alpha_1), v_2 f(\alpha_2), ..., v_n f(\alpha_n) | f(x) \in F[x]_k\}$$

- $F = \mathbb{F}_{64}$.
- $\hat{v} = (\texttt{!}, \texttt{!}, ..., \texttt{!})$.
- $\hat{\alpha} = (\texttt{A}, \texttt{B}, ..., \texttt{W})$.
- $f(x)$ is our *message polynomial*.

Message Polynomial

The message: "THIS IS MAJOR TOM".

$$f(x) = \boxed{\mathtt{T}} + \boxed{\mathtt{H}}\,x + \boxed{\mathtt{I}}\,x^2 + \boxed{\mathtt{S}}\,x^3 + \boxed{\phantom{\mathtt{M}}}\,x^4 + \boxed{\mathtt{I}}\,x^5 + \boxed{\mathtt{S}}\,x^6 + \boxed{\phantom{\mathtt{M}}}\,x^7 + \boxed{\mathtt{M}}\,x^8 + \boxed{\mathtt{A}}\,x^9 + \boxed{\mathtt{J}}\,x^{10} + \boxed{\mathtt{O}}\,x^{11} + \boxed{\mathtt{R}}\,x^{12} + \boxed{\phantom{\mathtt{M}}}\,x^{13} + \boxed{\mathtt{T}}\,x^{14} + \boxed{\mathtt{O}}\,x^{15} + \boxed{\mathtt{M}}\,x^{16}$$

The Codeword

The codeword, $\hat{c} = (v_1 f(\alpha_1), v_2 f(\alpha_2), \ldots, v_n f(\alpha_n))$

$$\hat{c} = (\texttt{!}\, f(\texttt{A}), \texttt{!}\, f(\texttt{B}), \ldots, \texttt{!}\, f(\texttt{W}))$$

$$\hat{c} = (\texttt{T}, \texttt{(}, \texttt{U}, \texttt{8}, \texttt{P}, \texttt{K}, \texttt{G}, \texttt{N}, \texttt{W}, \texttt{P}, \texttt{4}, \texttt{K}, \texttt{'}, \texttt{\_}, \texttt{N}, \texttt{(}, \texttt{M}, \texttt{H}, \texttt{K}, \texttt{1}, \texttt{"}, \texttt{<}, \texttt{K})$$

The Received Message

$$\hat{c} = (\texttt{T}, \texttt{(}, \texttt{U}, \texttt{8}, \texttt{P}, \texttt{K}, \texttt{G}, \texttt{N}, \texttt{W}, \texttt{P}, \texttt{4}, \texttt{K}, \texttt{'}, \textvisiblespace, \texttt{N}, \texttt{(}, \texttt{M}, \texttt{H}, \texttt{K}, \texttt{1}, \texttt{"}, \texttt{<}, \texttt{K})$$

$$\hat{p} = (\texttt{T}, \texttt{(}, \texttt{U}, \texttt{8}, \texttt{P}, \texttt{K}, \texttt{Z}, \texttt{N}, \texttt{W}, \texttt{P}, \texttt{\&}, \texttt{K}, \texttt{'}, \textvisiblespace, \texttt{N}, \texttt{(}, \texttt{M}, \texttt{H}, \texttt{K}, \texttt{1}, \texttt{"}, \texttt{R}, \texttt{K})$$

$$\hat{c} = \hat{p} + \hat{e}$$

Theorem

In [1], Hall states that there exists $\hat{u} = (u_1, u_2, \ldots, u_n)$ satisfying the following condition:

$$\sum_{i=1}^{n} \frac{c_i u_i}{1-\alpha_i z} = 0 \bmod z^r$$

Where $r = n - k$.

Calculating $\hat{u}$

$$L(x) = (x - \alpha_1)(x - \alpha_2)...(x - \alpha_n)$$

$$L_i(x) = \frac{L(x)}{(x - \alpha_i)}$$

$$\hat{u} = (L_1(\alpha_1), L_2(\alpha_2), ...L_n(\alpha_n),)$$

$$\hat{u} = (L_1(\boxed{\texttt{A}}), L_2(\boxed{\texttt{B}}), ...L_{23}(\boxed{\texttt{W}}))$$

$$\begin{aligned}\hat{u} = (&\boxed{\texttt{2}}, \boxed{\texttt{D}}, \boxed{\texttt{V}}, \boxed{\texttt{+}}, \boxed{\texttt{9}}, \boxed{\texttt{0}}, \boxed{\texttt{]}}, \boxed{\texttt{G}}, \boxed{\texttt{*}}, \boxed{\texttt{\^{}}}, \boxed{\texttt{3}}\\ &\boxed{\texttt{5}}, \boxed{\texttt{X}}, \boxed{\texttt{,}}, \boxed{\texttt{A}}, \boxed{\texttt{A}}, \boxed{\texttt{>}}, \boxed{\texttt{<}}, \boxed{\texttt{C}}, \boxed{\texttt{8}}, \boxed{\texttt{G}}, \boxed{\texttt{E}}, \boxed{\texttt{:}})\end{aligned}$$

Finding the Syndrome Polynomial

We now must calculate the Syndrome Polynomial, $S_p(z)$.

$$S_p(z) = \sum_{i=1}^{n} \frac{p_i u_i}{1-\alpha_i z} (\text{mod } z^r)$$

$$S_p(z) = \boxed{\texttt{?}} + \boxed{\texttt{V}}\, z + \boxed{\texttt{9}}\, z^2 + \boxed{\texttt{+}}\, z^3 + \boxed{\texttt{\^{}}}\, z^4 + \boxed{\texttt{1}}\, z^5 \text{ mod } z^6$$

Theorem

J. Hall states in [1] that:

Given r and $S_p(z) \in F[z]$ there is at most one pair of polynomials $\sigma(z), \omega(z) \in F[z]$ satisfying:

- $\sigma(z)S_p(z) = \omega(z) \bmod z^r$
- $\deg(\sigma(z)) \leq r/2$ and $\deg(\omega(z)) < r/2$
- $\gcd(\sigma(z), \omega(z)) = 1$ and $\sigma(0) = 1$

Introducing $\sigma(z)$ and $\omega(z)$

$\sigma(z)$ is called the error locator polynomial

$\omega(z)$ is called the error evaluator polynomial

The Euclidean Algorithm

Due to the previous theorem, and another theorem from [1], we can use the Euclidean Algorithm to find $\sigma(z)$ and $\omega(z)$.

Step i	$q_i(z)$	$r_i(z)$	$s_i(z)$	$t_i(z)$
-1	–	$\texttt{!}\,z^6$	$\texttt{!}$	$\square$
0	–	$S_p(z)$	$\square$	$\texttt{!}$
1	$\texttt{8} + \texttt{V}\,z$	$\texttt{\$} + \texttt{\$}\,z + \texttt{\_}\,z^2 + \texttt{6}\,z^3 + \texttt{K}\,z^4$	$\texttt{!}$	$\texttt{8} + \texttt{V}\,z$
2	$\texttt{X} + \texttt{6}\,z$	$\texttt{Z} + \texttt{(}\,z + \texttt{3}\,z^2 + \texttt{J}\,z^3$	$\texttt{X} + \texttt{6}\,z$	$\texttt{:} + \texttt{Y}\,z + \texttt{\%}\,z^2$
3	$\texttt{C} + \texttt{Q}\,z$	$\texttt{N} + \texttt{\_}\,z + \texttt{S}\,z^2$	$\texttt{N} + \texttt{I}\,z + \texttt{D}\,z^2$	$\texttt{A} + \texttt{=}\,z + \texttt{6}\,z^2 + \texttt{P}\,z^3$

$$\sigma(z) = t_3(\square)^{-1} t_3(z) = \texttt{!} + \texttt{Z}\,x + \texttt{L}\,x^2 + \texttt{C}\,x^3$$

$$\omega(z) = t_3(\square)^{-1} r_3(z) = \texttt{?} + \texttt{]} + \texttt{E}\,x^2$$

Finding the Error Locations

The set of error locations, B, is defined as: $B = \{b | \sigma(\alpha_b^{-1}) = 0\}$

$\sigma(z) = \boxed{\texttt{!}} + \boxed{\texttt{Z}}x + \boxed{\texttt{L}}x^2 + \boxed{\texttt{C}}x^3$

The roots of σ are: $\boxed{\texttt{3}}, \boxed{\texttt{\%}}, \boxed{\texttt{1}}$

The inverses of the roots are: $\boxed{\texttt{G}}, \boxed{\texttt{K}}, \boxed{\texttt{V}}$ which correspond to the positions 7, 11, and 22 in $\hat{\alpha}$

$B = \{7, 11, 22\}$

Finding the Error Values

The error value e_b where $b \in B$ was defined in [1] as:

$$e_b = \frac{-\alpha_b \omega(\alpha_b^{-1})}{u_b \sigma'(\alpha_b^{-1})}$$

$$e_7 = \frac{\mathtt{G}\, \omega(\mathtt{3})}{\mathtt{]}\, \sigma'(\mathtt{3})} = \mathtt{=}$$

$$e_{11} = \frac{\mathtt{K}\, \omega(\mathtt{\%})}{\mathtt{3}\, \sigma'(\mathtt{\%})} = \mathtt{2}$$

$$e_{22} = \frac{\mathtt{V}\, \omega(\mathtt{1})}{\mathtt{E}\, \sigma'(\mathtt{1})} = \mathtt{N}$$

$$\hat{e} = (, , , , , , \mathtt{=}, , , , \mathtt{2}, , , , , , , , , , , \mathtt{N},)$$

Correcting the Errors

$$\hat{p} = (\texttt{T}, \texttt{(}, \texttt{U}, \texttt{8}, \texttt{P}, \texttt{K}, \texttt{Z}, \texttt{N}, \texttt{W}, \texttt{P}, \texttt{\&}, \texttt{K}, \texttt{'}, \texttt{\_}, \texttt{N}, \texttt{(}, \texttt{M}, \texttt{H}, \texttt{K}, \texttt{1}, \texttt{"}, \texttt{R}, \texttt{K})$$

$$\hat{e} = (\square, \square, \square, \square, \square, \square, \texttt{=}, \square, \square, \square, \texttt{2}, \square, \square, \square, \square, \square, \square, \square, \square, \square, \square, \texttt{N}, \square)$$

$$\hat{c} = (\texttt{T}, \texttt{(}, \texttt{U}, \texttt{8}, \texttt{P}, \texttt{K}, \texttt{G}, \texttt{N}, \texttt{W}, \texttt{P}, \texttt{4}, \texttt{K}, \texttt{'}, \texttt{\_}, \texttt{N}, \texttt{(}, \texttt{M}, \texttt{H}, \texttt{K}, \texttt{1}, \texttt{"}, \texttt{<}, \texttt{K})$$

Outline

1 Defining the Playing Field

2 Codes

3 Generalized Reed-Solomon Codes

4 Conclusion

References

J.I. Hall.
Notes on Coding Theory.
Michigan State University, 2012.

I.S. Reed and G Solomon.
Polynomial codes over certain finite fields.
Journal of the Society for Industrial and Applied Mathematics, 8:300–304, June 1960.

B Sklar.
Reed solmon codes.
2001.

Questions