DMP221
Discrete Mathematics
Final Exam – Form A

120 Minutes

Instructions:

- **The exam consists of 12 problems on 3 pages. Most problems are subdivided into sections like 1(a), 1(b), etc. The last problem is 12. Make sure your exam is complete before you begin.**
- **Show all work in detail or your answer will not receive any credit. All answers without supporting work receive ZERO credit.**
- **Write neatly and box all answers.**
- **Include appropriate units on all questions that apply. When drawing graphs, make sure to clearly label axes, scale, and curves.**
- **Do not use your own scratch paper. You may ask for scratch paper at the front desk (or from your instructor if the exam is conducted in class). • Turn off your handy phone. Leave all electronic devices in your backpack, and leave your backpack at the front of the room. • No calculators with QWERTY keyboards or ones like the Casio FX-2, TI-89 or TI-92 that do symbolic algebra may be used.**
- **Add your student ID, name, signature and submit this form together with your answer sheet.**

Honor Statement:
By signing below you confirm that you have neither given nor received any unauthorized assistance on this exam. This includes any use of a graphing calculator beyond those uses specifically authorized by the Faculty of Information Technology (FIT) and your instructor. Furthermore, you agree not to discuss this exam with anyone until the exam testing period is over. In addition, your calculator's program memory and menus may be checked at any time and cleared by any testing center proctor or FIT's instructor.

_____ _____ _____

Student ID Student Name Signature

DMP221–Discrete Mathematics, Spring 2013, Final Exam – Form A, 120 Minutes©c 2013
Hanoi University, Faculty of Information Technology

1. (5 points) Prove the theorem: "There are no rational number solutions to the equation $x^3 + x + 1 = 0$." by contradiction.

2. (10 points) Which of these sentences are propositions? What are the truth values of those that are propositions?

   (a) $1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \ldots + \frac{1}{\sqrt{n}} > \sqrt{n}, \ (\forall n \in \mathbb{Z}, n \geq 2).$

   (b) $3 + 9 + 27 + \ldots + 3^n = \frac{1}{2}(3^{n+1} - 3), \ (\forall n \in \mathbb{Z}, n \geq 1)$.

3. (10 points) Find x in the following equations:

   (a) $21x \equiv 7 \pmod{28}$. (b) $13x \equiv 1 \pmod{29}$.

4. (5 points) Find the function that goes through the points (3,1), (4,2) and (5,3) by using Lagrange interpolation method.

5. (10 points) Suppose you are in charge of setting up a secret sharing scheme where you want to distribute $n = 5$ shares to 5 people such that any $k = 3$ or more people can figure out the secret, but 2 or fewer cannot. Lets say we are working over $GF(7)$ and you randomly choose the polynomial of degree $k - 1 = 2$,$P(x) = 3x^2 + 5x + 1$ (here, $P(0) = 1 = s$, the secret). Well, the shares handed out are $P(1) = 2$ to the first official, $P(2) = 2$ to the second, $P(3) = 1$ to the third, $P(4) = 6$ to the fourth, and $P(5) = 3$ to the fifth official. Lets say that officials 3, 4, and 5 get together (we expect them to be able to recover the secret). Using Lagrange interpolation, they compute the following delta functions:

   $$\triangle_3(x) = \frac{(x-4)(x-5)}{2}, \ \triangle_4(x) = \frac{(x-3)(x-5)}{-1}, \ \triangle_5(x) = \frac{(x-3)(x-4)}{2}.$$

   They then compute the polynomial over $GF(7)$ to get $P^*(x)$ as follows:

   $$P^*(x) = (1)\triangle_3(x) + (6)\triangle_4(x) + (3)\triangle_5(x) = 3x^2 + 5x + 1.$$

   Now they simply compute $P^*(0)$ and discover that the secret is 1. If officials 1, 2, and 5 get together, we will obtain a different $P^\dagger(x)$. Prove that $P^\dagger(x) \Leftrightarrow P^*(x)$ over $GF(7)$.

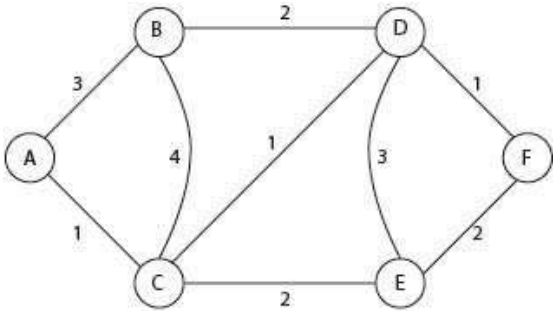
6. (10 points) We received data through a transmission line with general error rate is 1 over 5 packages. The received packages are: {2,0,6,0,3}.

   (a) Which package has been changed?

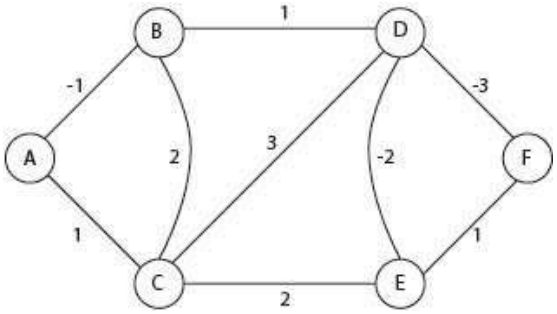
(b) What is the corrected value of the error package?

Knowing that the encryption employed polynomials over $GF(29)$.

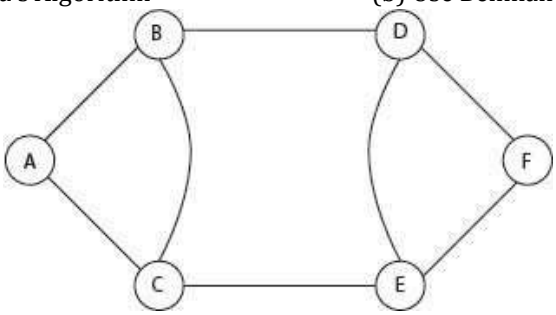
7. (10 points) Using Dijkstra's algorithm, find the shortest path from A to all other vertices in the Figure 1(a).
8. (10 points) Using Bellman-Ford's algorithm, find the shortest path from C to all other vertices in the Figure 1(b).
9. (10 points) Using Depth-First-Search's algorithm, show visiting process and the final level graph with starting vertex is E in the Figure 1(c).
10. (10 points) Using Breadth-First-Search's algorithm, show visiting process and the final level graph with starting vertex is B in the Figure 1(c).



(a) Use Dijkstra's Algorithm



(b) Use Bellman-Ford's Algorithm



(c) Use DFS & BFS Algorithms

Figure 1: Graphs

11. (5 points) Explain three types of traversal in binary trees.
12. (5 points) Create a matrix representation for the relation

$R = \{(a,b) : a - 1 < b\}$ where $a \in A = \{1,3,5,7\}, b \in B = \{2,4,6,8\}$.

3

DMP221
Discrete Mathematics – Fall 2013
Final Exam – Form B – Solution

120 Minutes

Instructions:

- **The exam consists of 7 problems on 7 pages. Most problems are subdivided into sections like 1(a), 1(b), etc. The last problem is 7b. Make sure your exam is complete before you begin.**
- **Show all work in detail or your answer will not receive any credit. All answers without supporting work receive ZERO credit.**
- **Write neatly and box all answers.**
- **Include appropriate units on all questions that apply. When drawing graphs, make sure to clearly label axes, scale, and curves.**
- **Do not use your own scratch paper. You may ask for scratch paper at the front desk (or from your instructor if the exam is conducted in class). • Turn off your handy phone. Leave all electronic devices in your backpack, and leave your backpack at the front of the room. • No calculators with QWERTY keyboards or ones like the Casio FX-2, TI-89 or TI-92 that do symbolic algebra may be used.**
- **Add your student ID, name, signature and submit this form together with your answer sheet.**

Honor Statement:

By signing below you confirm that you have neither given nor received any unauthorized assistance on this exam. This includes any use of a graphing calculator beyond those uses specifically authorized by the Faculty of Information Technology (FIT) and your instructor. Furthermore, you agree not to discuss this exam with anyone until the exam testing period is over. In addition, your calculator's program memory and menus may be checked at any time and cleared by any testing center proctor or FIT's instructor.

_____	_____	_____
Student ID	Student Name	Signature

1. **Multiple Choices (20 points):** Select the best answer for the question.

(a) (2 points) The implication $q \to \neg p$ is true for all possible assignments of truth values to p and q except for which assignment?

i. p true, q true. ii. p true, q false. iii. p false, q true. iv. p false, q false.

(b) (2 points) Which of the following is the negation of "No one plays tennis"?

i. Everyone plays tennis. iii. Someone does not play tennis.
ii. Someone plays tennis. iv. Anyone can play tennis.

(c) (2 points) Which of the following is the negation of $\forall x(P(x) \to Q(x))$?

i. $\exists x\,(P(x) \to Q(x))$ iii. $\exists x\,(\neg P(x) \to \neg Q(x))$
ii. $\exists x\,(P(x) \wedge \neg Q(x))$ iv. $\exists x\,(\neg P(x) \wedge Q(x))$

(d) (2 points) Express the following statement in symbols:

"Between every two distinct real numbers there is a third real number."

In the following choices, assume that the universe for a,b and c consists of all numbers.

i. $\forall a \forall b \exists c\,((a \neq b) \to (a < c < b))$. ii. $\forall a \forall b \exists c\,((a < c < b) \vee (b < c < a))$.

iii. $\forall a \forall b \exists c\,[(a \neq b) \to ((a < c < b) \vee (b < c < a))]$.

iv. $\exists a \exists b \exists c\,((a < c < b) \vee (b < c < a))$.

v. $\exists c \forall a \forall b\,(a < c < b)$.

(e) (2 points) Suppose f: **R** → **R** has the rule $f(x) = \left\lfloor \frac{x}{2} \right\rfloor$ and suppose g : **R** → **R** has the rule $g(x) = \lceil \frac{5 - 2x}{3} \rceil$. Find $(f \circ g)(5)$.

i. 1. ii. -1 iii. 0. iv. none of these.

(f) (2 points) Which statement about the function $f(x) = x^2 + 1$ from the set of integers to the set of positive integers is correct?

i. $f(x)$ is one-to-one and onto.
iv. $f(x)$ is neither one-to-one nor onto.
ii. $f(x)$ is onto, but not one-to-one.
iii. $f(x)$ is one-to-one, but not onto.

(g) (2 points) If $S \subseteq T$, then

i. $\overline{T} \subseteq \overline{S}$. iv.. ii. $T \subseteq S \cap T$. v. iii. $T - S$ $\begin{matrix} T - S \subseteq S - T \\ S \cup T = S \cap T. \end{matrix}$ $\neq \emptyset$.

(h) (2 points) Let $P(n)$ be the statement "you can make n cents postage using 3cent and 5-cent stamps." Suppose you want to use the principle of mathematical induction to show that $P(n)$ is true for all $n \geq 8$.

You begin by proving $P(8)$, which is true because 8 cents postage can be made with one 3-cent stamp and one 5-cent stamp. Which of the following will show that the implication $P(k) \rightarrow P(k + 1)$ in the inductive step is true for all $k \geq 8$?

i. Take the stamps that are used to make k cents postage and add a 3-cent stamp.
ii. Take the stamps that are used to make k cents postage and add a 5-cent stamp.
iii. Take the stamps that are used to make k cents postage, remove a 5-cent stamp and add a 3-cent stamp.
iv. Take the stamps that are used to make k cents postage, remove three 3-cent stamp and add two 5-cent stamps.
v. None of these.

(i) (2 points) Let R be a set, with two operations addition ($a,b \rightarrow 7\ a + b$) and multiplication ($a,b\ 7\rightarrow a \times b$) are defined where $a,b \in R$. $(R,+,\times)$ will be a ring if the following holds:

i. Closure, associate law, identity element, inverse element.
ii. Closure, associate law, commutative law, distributive law, additive identity element, additive inverse element.
iii. Closure, associative law, commutative law, distributive law, additive identity element, additive inverse element, multiplicative identity element, multiplicative inverse element.
iv. Closure, associative law, commutative law, distributive law, multiplicative identity element, multiplicative inverse element.

(j) (2 points) Alice set up a secret sharing scheme where she want to distribute five shares to five persons such that any three or more persons can figure out the secret, but two or fewer persons cannot. She employs the polynomial $P(x)$ in $GF(7)$ (where $P(0) = s$ is the secret) with the shares are $P(1) = 4$, $P(2) = 5$, $P(3) = 1$, $P(4) = 6$, and $P(5) = 6$. So, the secrete key must be

i. 2 ii. 3 iii. 5 iv. 4

Solution: $(a).i;(b).ii;(c).ii;(d).iii;(e).ii;(f).iv;(g).i;(h).v;(i).ii;(j).iii$ – $P(x) = x^2 - 2x + 5$

Check Self Assessments link in DMP course.

2. **Fill in the Blank (30 points):** Use only one word for each question.

(a) (2 points) A _____ is a sequence of edges that begins at a vertex of a graph and travels from vertex to vertex along edges of the graph. (path)

(b) (2 points) The set of all neighbors of a vertex v of $G = (V,E)$, denoted by $N(v)$, is called the _____ of v. If A is a subset of V , we denote by $N(A)$ the set of all vertices in G that are adjacent to at least one vertex in A. So, $N(A) = \cup_{v \in A} N(v)$. (neighborhood)

(c) (2 points) Let $G = (V,E)$ be an undirected graph with m edges. Then $2m = \sum_{v \in V} \deg(v)$ is the _____ theorem. (handshaking)

(d) (2 points) An _____path in G is a simple path containing every edge of G. (Euler)

(e) (2 points) _____ paths and circuits can be used to solve practical problems. For example, many applications ask for a path or circuit that visits each road intersection in a city, each place pipelines intersect in a utility grid, or each node in a communications network exactly once. Finding a _____ path or circuit in the appropriate graph model can solve such problems. The famous traveling salesperson problem or TSP (also known in older literature as the traveling salesman problem) asks for the shortest route a traveling salesperson should take to visit a set of cities. This problem reduces to finding a _____ circuit in a

complete graph such that the total weight of its edges is as small as possible. (Hamilton)

(f) (2 points) The _____ number of a graph is the least number of colors needed for a coloring of this graph. The _____ number of a graph G is denoted by $\chi(G)$. (Here χ is the Greek letter *chi*.) (chromatic)

(g) (2 points) A relation R on a set A is called _____ if $(a,a) \in R$ for every element $a \in A$. (reflexive)

(h) (2 points) A path or circuit is called _____ if it does not contain the same edge more than once. (simple)

(i) (2 points) A _____ is a connected undirected graph with no simple circuits. (tree)

(j) (2 points) Let G be a simple graph. A spanning tree of G is a subgraph of G that is a tree containing _____ vertex of G. (every)

(k) (2 points) Early 18th century, a _____ mathematician studied the "matching problem". (French)

(l) (2 points) A Latin square of order n is an $n \times n$ matrix whose entries are the integers 1,2,...,n, arranged so that each integer appears exactly _____ in each row and exactly _____ in each column. (once)

(m) (2 points) The idea behind the Hungarian method is to try to transform a given _____ problem specified by C into another one specified by a matrix $\hat{C} = [\hat{c}_{ij}]$, such that $\hat{c}_{ij} \geq 0$, for all pairs i,j, where both problems have the same set of optimal solutions. (assignment)

(n) (2 points) A clique in a graph G is a _____ of G that is a complete graph. (subgraph)

(o) (2 points) The maximum flow from vertex s to vertex $t \neq s$ in a directed graph G with capacities on its edges is less than or equal to the capacity of any _____ $(A, V(G) - A)$ having $s \in A$ and $t \notin A$. (cut)

Questions 2.(k) to 2.(o): 2nd round projects.

3. **Congruence (10 points):** Find x in the following equations:

(a) (5 points) $27^{x} \equiv 24 \pmod{33}$. $(gcd(27,33) = 3; x_0 = 7; x = x_0 + k\frac{33}{3} = 7, 18, 29)$

(b) (5 points) $37x \equiv 1 \pmod{51}$. ($x = 40$)

4. **RSA or Error Correcting Code (10 points):** Select only ONE question to solve

(a) (10 points) What is the original message encrypted using the RSA system with $p = 5, q = 11$ and $e = 17$ and the codes of the encrypted message is 48 06 07. (Student must use the ASCII tables to look up the ASCII codes and find the characters.) ($d = 33, m$ = 53 'Start of text'. ASCII code: 53 51 02)

(b) (10 points) We received data through a transmission line with general error rate is 1 over 5 packages. The received packages are {5,0,4,4,4} and the encryption employs polynomials over $GF(7)$.

i. Which package has been changed? (Package 4)

ii. What is the corrected value of the error package? ($^{3\ 2}$ $P(x) = x^2 - x + 5; Q(x)$

□ □

$= x + 2x + 2x + 1;$ □□□□ −– □□□□□□

5/12
17/12 *x*
=11/12 ;
17/4
5/3

DMP221–Discrete Mathematics, Fall 2013, Final Exam – Form B – Solution, 120 Minutes ⓒc 2013
Hanoi University, Faculty of Information Technology

corrected value is 3.)

5. **Shortest Path Algorithms (10 points):** find the shortest path from A to all other vertices by using

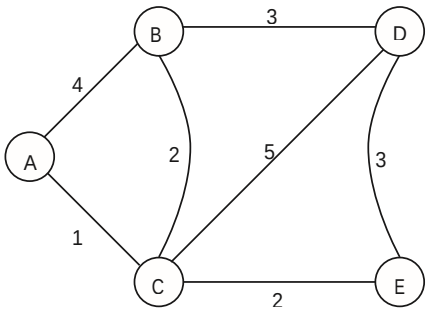
   (a) (5 points) Dijkstra's algorithm in the Figure 1(a)

   (b) (5 points) Bellman-Ford's algorithm in the Figure 1(b).

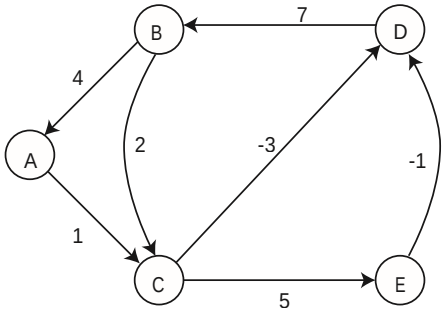
6. **Search Algorithms (10 points):** Start from vertex A in the Figure 1(c), show visiting process and the final level graph by using

   (a) (5 points) Depth-First-Search (DFS) algorithm with in-order traversal (left, root, right).

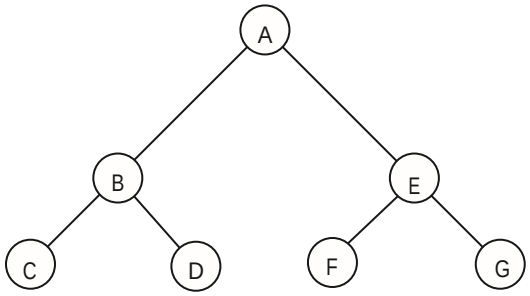
   (b) (5 points) Breadth-First-Search (BFS) algorithm.



(a)UseDijkstra'sAlgorithm



(b)UseBellman-Ford'sAlgorithm



(c)UseDFS&BFSAlgorithms

Figure 1: Graphs

7. **Binary Tree Application (10 points):** Given a data source with 8 characters A,B,C,D,E,F with probability of appearance as follows:

A	B	C	D	E	F
0.24	0.16	0.30	0.10	0.11	0.09

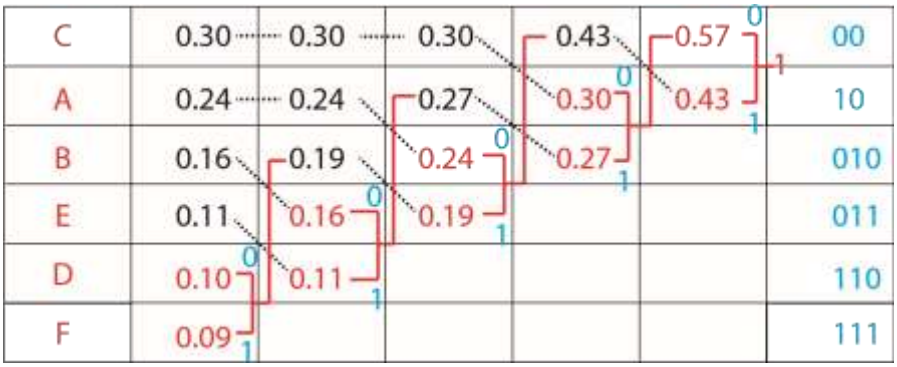
(a) (5 points) Encode the source and find the codewords for those characters. Draw the Huffman tree.

(b) (5 points) Calculate the average length of codewords ($\overline{L}$) and the entropy (H) of the source by the following equations:

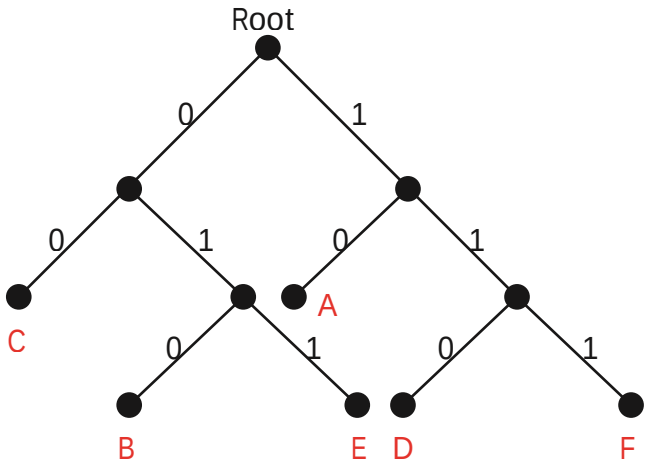
$$\overline{L} = \sum_{i=1}^{m} L_i \times p_i; \quad H = \sum_{i=1}^{m} p_i \times \log_2\left(\frac{1}{p_i}\right)$$

where m is number of different characters, L_i and p_i are length and probability of the ith codeword.

Solution:



(a) Encode



(b) Huffman tree

Figure 2: ASCII Table

$$\begin{aligned}
\overline{L} &= 0.30 \times 2 + 0.24 \times 2 + 0.16 \times 3 + 0.11 \times 3 + 0.1 \times 3 + 0.09 \times 3 = 2.\\
H &= 0.30 \times \log_2 \frac{1}{0.30} + 0.24 \times \log_2 \frac{1}{0.24} + 0.16 \times \log_2 \frac{1}{0.16}\\
&\quad +0.11 \times \log_2 \frac{1}{0.11} + 0.1 \times \log_2 \frac{1}{0.1} + 0.09 \times \log_2 \frac{1}{0.09} = 2.4334.
\end{aligned}$$

46;

Notes:

- Use ASCII Table (Figure 3) for question 4.a

- Use this inverse matrix for question 4.b

$$A^{-1} = \begin{pmatrix} -1/15 & -1/60 & 13/60 & -7/60 & -1/60 \\ 1/3 & 1/12 & -7/12 & -5/12 & 7/12 \\ -1/3 & -1/12 & 1/12 & 5/12 & -1/12 \\ -3/5 & 17/20 & 39/20 & 19/20 & -43/20 \\ 1/3 & -1/6 & -1/3 & -1/6 & 1/3 \end{pmatrix}$$

Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
0	00	Null	32	20	Space	64	40	@	96	60	`
1	01	Start of heading	33	21	!	65	41	A	97	61	a
2	02	Start of text	34	22	"	66	42	B	98	62	b
3	03	End of text	35	23	#	67	43	C	99	63	c
4	04	End of transmit	36	24	$	68	44	D	100	64	d
5	05	Enquiry	37	25	%	69	45	E	101	65	e
6	06	Acknowledge	38	26	&	70	46	F	102	66	f
7	07	Audible bell	39	27	'	71	47	G	103	67	g
8	08	Backspace	40	28	(	72	48	H	104	68	h
9	09	Horizontal tab	41	29	)	73	49	I	105	69	i
10	0A	Line feed	42	2A	*	74	4A	J	106	6A	j
11	0B	Vertical tab	43	2B	+	75	4B	K	107	6B	k
12	0C	Form feed	44	2C	,	76	4C	L	108	6C	l
13	0D	Carriage return	45	2D	-	77	4D	M	109	6D	m
14	0E	Shift out	46	2E	.	78	4E	N	110	6E	n
15	0F	Shift in	47	2F	/	79	4F	O	111	6F	o
16	10	Data link escape	48	30	0	80	50	P	112	70	p
17	11	Device control 1	49	31	1	81	51	Q	113	71	q
18	12	Device control 2	50	32	2	82	52	R	114	72	r
19	13	Device control 3	51	33	3	83	53	S	115	73	s
20	14	Device control 4	52	34	4	84	54	T	116	74	t
21	15	Neg. acknowledge	53	35	5	85	55	U	117	75	u
22	16	Synchronous idle	54	36	6	86	56	V	118	76	v
23	17	End trans. block	55	37	7	87	57	W	119	77	w
24	18	Cancel	56	38	8	88	58	X	120	78	x
25	19	End of medium	57	39	9	89	59	Y	121	79	y
26	1A	Substitution	58	3A	:	90	5A	Z	122	7A	z
27	1B	Escape	59	3B	;	91	5B	[	123	7B	{
28	1C	File separator	60	3C	<	92	5C	\	124	7C	|
29	1D	Group separator	61	3D	=	93	5D	]	125	7D	}
30	1E	Record separator	62	3E	>	94	5E	^	126	7E	~
31	1F	Unit separator	63	3F	?	95	5F	_	127	7F	□

(a) Code 0 → 127

Figure 3: ASCII Table