CPSC 536F, 2022: HOMEWORK SET 1

JOEL FRIEDMAN

Last revised: Thursday 24th March, 2022, at 09:19

You may work on homework in groups, **but you must write up your own solutions individually and must acknowledge with whom you worked.** You must also acknowledge any sources you have used beyond the textbooks and other course references. You must use the notation we use in class and/or the course references.

(1) In this exercise, logarithms are base e. Explain why the fact that $f(x) = \log(x)$ is monotone gives

$$\log(1) + \cdots + \log(n-1) \le \int_{t=1}^{n} \log(t)\ \mathrm{d}t \le \log(2) + \cdots + \log(n)$$

Use this to show $(n/e)^n \le n! \le (n/e)^n n$.

(2) In this exercise, logarithms are base e. Assume that $f\colon \mathbb{R} \to \mathbb{R}$ is twice continuously differentiable.

(a) Show for any $x_0 \in \mathbb{R}$, the function

$$F(h) = -2hf(x_0) + \int_{t=x_0-h}^{t=x_0+h} f(t)\,dt$$

satisfies $F(0) = F'(0) = F''(0) = 0$ and $F'''(h) = f''(x_0 - h) + f''(x_0 + h)$.

(b) Use Taylor's theorem to conclude the "midpoint rule,"

$$\int_{t=x_0-h}^{t=x_0+h} f(t)\,dt = 2hf(x_0) + (1/3)h^2 f''(\xi)$$

for some $\xi \in [x_0 - h, x_0 + h]$.

(c) Estimate

$$\int_{t=1/2}^{t=n+(1/2)} \log(t)\,dt$$

using the midpoint rule to show that for some constants $c_1, c_2 > 0$ we have

$$c_1(n/e)^n\sqrt{n} \le n! \le c_2(n/e)^n\sqrt{n}.$$

Research supported in part by an NSERC grant.

(d) From Taylor's theorem we have $|x| \le 1/2$ we have $\log(1+x) = x + O(x^2)$. Use this to show that for any constant C, the series

$$g(n) = \prod_{m=1}^{n} (1 + C/m^2) = (1+C)(1+C/4)(1+C/9)\dots(1+C/n^2)$$

has a finite limit, and, similarly,

$$h(n) = \prod_{m \ge C+1}^{n} (1 - C/m^2)$$

has a finite limit.

(e) Show that if $f(n) = n!/(n^{1/2}(n/e)^n)$, then $f(n+1)/f(n) = 1 + O(1/n^2)$.

(f) Conclude that for some constant $c > 0$ we have $n! \sim c\sqrt{n}(n/e)^n$, i.e.,

$$\lim_{n\to\infty} \frac{n!}{c\sqrt{n}(n/e)^n} = 1$$

(3) The Central Limit Theorem (typically proven using Fourier analysis) implies that for any real $a < b$, if $X_1, \dots, X_n$ are n independent random variables, each set to $0, 1$ with probability $1/2$ then the probability, then

$$\int_a^b \frac{1}{\sqrt{2\pi}} e^{-x^2/2}\, dx$$

equals the limit as $n \to \infty$ of that probability that

$$a \le \frac{X_1 + \dots + X_n - n\mu}{\sigma\sqrt{n}} \le b$$

where $\mu = 1/2$ (i.e., the average value of each X_i) and $\sigma = 1/2$ (i.e., the variance of each X_i, i.e., the square root of the expected value of $(X_i - 1/2)^2$). Taking $a < 0 < b$ and both a, b near 0, show that the previous exercise implies that $n! \sim c\sqrt{n}(n/e)^n$ where $c = \sqrt{2\pi}$.

(4) Consider the number, $C = C(s,n)$ of circuits of size s in Boolean variables $x_1, \dots, x_n$ over the gates $\vee, \wedge, \neg$. In other words, we can wiew a circuit as a "straight-line program," with $y_1, \dots, y_s$ where $y_i = x_i$ for $i \le n$, and for $i \ge n+1$ there are $j, k < i$ such that either (1) $y_i = \neg y_j$, (2) $y_i = y_j \vee y_k$, (3) $y_i = y_j \wedge y_k$. Since for $i \ge n+1$ there are $i-1$ choices for (1), and $\binom{i-1}{2}$ for (2) and (3), we conclude that $C(i,n) \le (i^2-1)C(i-1,n)$.

(a) Using the simpler estimate $C(i,n) \le i^2 C(i-1,n)$ we can conclude that

$$C(s,n) \le \big((n+1)(n+2)\cdots s\big)^2.$$

Use this to show that for large n, most Boolean functions on n-variables require circuits of size $c(2^n/n)$ for some constant c.

(b) If we use the cruder but simpler bound $C(i,n) \le s^2 C(i-1,n)$ for $i \le s$, we get

$$C(s,n) \le (s^2)^s.$$

If we use this cruder bound to show that most Boolean functions on n-variables require circuits of size $c'(2^n/n)$ for some constant c', do we get the same constant c' as c in the previous item? Explain.

(5) Let $T(n)$ be the number of binary trees on n. Setting $T(1) = 1$ we explained why

$$T(n) \leq T(1)T(n-1) + T(2)T(n-2) + \cdots + T(n-1)T(1).$$

(a) Does this inequality still hold for the number of arbitrary trees on n leaves?

(b) Find a formula for the sequence T defined by $T(1) = 1$ and for $n \geq 2$,

$$T(n) = T(1)T(n-1) + T(2)T(n-2) + \cdots + T(n)T(1).$$

Do this by setting

$$G(z) = \sum_{n=1} z^n T(n)$$

as a formal power series $G(z)$ that satisfies $(G(z))^2 = G(z) - z$, and hence $G^2 - G + z = 0$ as formal power series.

(i) Argue that $T(n) \leq c^n$ for some $c > 0$. [Hint: you can argue that $T(n)$ equals the number of sequences of $2n$ of matching left and right parenthesis, and hence $T(n) \leq 2^{2n}$].

(ii) Use this to argue that $G(z)$ is a convergent series for $|z|$ sufficiently small, and hence for all sufficiently small $|z|$,

$$G(z) = \frac{1 \pm \sqrt{1-4z}}{2}.$$

(iii) Expand $(1-4z)^{1/2}$ as a power series near $z = 0$ (via Taylor's theorem) to find a simple formula for $T(n)$. [You are implicitly using the theorem that if $G_1(z)$ and $G_2(z)$ are formally power series that both converge for $|z|$ sufficiently small, then G_1, G_2 are the same power series iff $G_1(z) = G_2(z)$ for all $|z|$ sufficiently small. You can assume this.]

(6) Consider Andreev's function on parameters N, ℓ given by (1) identifying functions $f\colon \{0,1\}^N \to \{0,1\}$ with an 2^N set of Boolean variables (arranged by the 2^N truth table values of f in some reasonable way), (2) letting $\mathbf{z}^1, \ldots, \mathbf{z}^\ell$ be Boolean variables of N-bits each, and (3) setting

$$A_{N,\ell}(f, \mathbf{z}^1, \ldots, z^\ell) = f(\mathbf{z}^1 \oplus \ldots \oplus \mathbf{z}^\ell).$$

Hence $A_{N,\ell}$ is a function of $2^N + N\ell$ variables. For these questions, for simplicity let N be a power of 2, set $n/2 = 2^N = N\ell$ so that $n = 2^{N+1}$ and $\ell = n/(2N) = 2^{N-\log_2 N}$ are integers. (And $A_{N,\ell}$ has $n/2$ variables describing f, and $n/2$ variables devoted to the $\mathbf{z}^i$'s.

In more detail, assume that we identifiy functions $f\colon \{0,1\}^N \to \{0,1\}$ with Boolean variables $x_0, \ldots, x_{2^N-1}$ where x_i is the value of $f(\text{baseTwo}(i))$ where baseTwo(i) is the N-bit base two representation of i viewed as an element of $\{0,1\}^N$.

(a) Show that $A_{N,\ell}$ above can be computed by a formula of size $O(n^3)$.

(b) In the $N\ell$ array of variables that $\mathbf{z}^1,\dots,\mathbf{z}^\ell$, the probability that a random choice of m variables entirely misses the i-th -component of $\mathbf{z}^1,\dots,\mathbf{z}^\ell$ for a fixed $i\in[N]$ is bounded by

$$\binom{N\ell-\ell}{m}\Big/\binom{N\ell}{m},$$

(c) Explain why if we randomly restrict all but m of the $n/2=N\ell$ variables amoung the $\mathbf{z}^1,\dots,\mathbf{z}^\ell$ to $\{0,1\}$, the probability that there exists a $j\in\{1,\dots,N\}$ such that all of the j-th components of $\mathbf{z}^1,\dots,\mathbf{z}^\ell$ have been restricted is at most

$$N\binom{N\ell-\ell}{m}\Big/\binom{N\ell}{m}. \tag{1}$$

(d) Show that for any three positive integers $p\le q\le r$,

$$(r/q)^p \le \binom{r}{p}\Big/\binom{q}{p} \le \big((r-p+1)/(q-p+1)\big)^p.$$

(e) Show that from some constant c, if we take $m=c(\log n)^2$ then the expression in (1) is less than $1/2$, and give an explicit c. [Hint: one way to do this is to bound the ratio of binomial coefficients from above using the previous part.]

(f) Say that we randomly restrict all but $m=c(\log n)^2$ of the variables in $\mathbf{z}^1,\dots,\mathbf{z}^\ell$ to $\{0,1\}$, and pick a particular choice of the N variables representing f, that a size L formula for $A_{N,\ell}$ must be of size at least $2^N/C\log_2(N)$ for some constant C.

(g) Say that we can prove that any formula of size L on n Boolean variables shrinks to size at most $L(m/n)^\gamma$ when we randomly choose all but m of the formula's variables and restrict their values to $0,1$ as in Subbotovskaya's result (of $\gamma=3/2$). Show that Andreev's $A_{N,\ell}$ with parameters as above requires formula size at least $c_1 n^{1+\gamma}/(\log n)^{c_2}$ for constants c_1,c_2 and n sufficiently large; give a value for c_2.

(7) Consider the following variant of Subbotovskaya's method: we take a formula of size L in n variables, randomly (uniformly) choose $n-m$ variables and restrict their values to be $0,1$ *in any way* (rather than each being independently set to $0,1$, each value with probability $1/2$), such that we can show L shrinks to size $CL(m/n)^\gamma$ for some constants C,γ. Does this change our conclusions regarding the parity function and Andreev's function?

(8) An *alternating AND/OR formula of depth d* we mean a De Morgan formula that is a complete binary tree of depth d, with $d\ge 2$ a positive even integer, such that the root has an AND gate, its two children have OR gates, and the AND and OR and or gates keeps alternating on each level (i.e., if a gate is of distance $d'<d$ to the root, then it is an AND gate if d' is even, and an OR gate if d' is odd). For example, an alternating AND/OR formula of depth 4 is a formula of the form:

$$(p_0\vee p_1)\wedge(p_2\vee p_3),$$

where for $i = 1, \ldots, 4$,

$$p_i = (z_{4i} \vee z_{4i+1}) \wedge (z_{4i+2} \vee z_{4i+3}),$$

and $z_0, \ldots, z_{15}$ are literals. Show that any function computed by De Morgan formula of depth D can also be computed by an alternating AND/OR fromula of depth at most $2D$.

(9) Recall that NAND is the Boolean function defined as $\text{NAND}(x_1, x_2) = \neg(x_1 \wedge x_2)$. Show that any fucntion computed by a De Morgan formula of depth d can be computed by a NAND formula of depth at most $2d$, i.e., a tree where only NAND gates are allowed (i.e., on the interior nodes) with literals on the leaves.

(10) (a) Show that any Boolean function $\{0,1\}^n \to \{0,1\}$ can be expressed by a formula of size $2^{n+1} - 2$ [1] [Hint: for $n = 1$ this is clear. Use induction, noting that a function $f = f(x_1, \ldots, x_n)$ can be written as x_1 and g or $\neg x_1$ and h, where g, h are functions of $x_2, \ldots, x_n$.]

(b) Show that the above strategy carries over to monotone Boolean functions and monotone Boolean formulas; i.e., show that any monotone Boolean function $\{0,1\}^n \to \{0,1\}$ can be expressed by a monotone formula (i.e., where the leaves are the variables $x_1, \ldots, x_n$ and we do not allow the negated variables $\neg x_1, \ldots, \neg x_n$) of size at most 2^{n-1}.

(11) Does Spira's lemma hold — in some modified form — for monotone Boolean functions and monotone Boolean formulas? Explain.

(12) In class we showed that for even n, the number of monotone Boolean functions $\{0,1\}^n \to \{0,1\}$ is at least 2^r where $r = \binom{n}{n/2}$ (a similar bound holds for n odd, with $n/2$ rounded up or down). Use this to show that for large n, most monotone Boolean funcitons are not expressed by formulas of size $c2^n/(n^{1/2} \log n)$ for some constant $c > 0$. [Hint: you can use the proof of the analogous result for general Boolean functions.]

(13) Show that there is no 4×4 matrix that satisfies the condition of a "Valiant gadget" where "permanent" is replaced with "determinant." In other words, show that there is no 4×4 matrix, X, that satisfies the following conditions: (i) $\det X = 0$, (ii) $\det X(1;1) = 0$, (iii) $\det X(4;4) = 0$, (iii) $\det X(1,4;1,4) = 0$, and (iii) $\det X(1;4) = \det X(4;1)$ is nonzero. (where we use $X(A;B)$ to denote X with the rows of A and columns of B removed). Show the same with 4 everywhere replaced by any integer greater than 4.

Department of Computer Science, University of British Columbia, Vancouver, BC V6T 1Z4, CANADA.

E-mail address: jf@cs.ubc.ca

URL: http://www.cs.ubc.ca/~jf

[1] This improvement to the stated bound in class was pointed out in 2022 by Victor Wang.