Требование к зачету

Для зачета нужно решить не меньше, чем a задач из части A, b задач из части B и c задач из части C и не менее, чем s задач всего. Если в задаче несколько пунктов, то нужно решить их все. Параметры a, b, c, s из таблицы:

Имя	a	b	c	s
Данил	0	0	2	3
Святослав	0	1	3	5
Артур	2	2	2	6
Настя	1	2	3	7
Таня	1	3	3	8
Надя	3	3	3	10
Марсель	6	1	3	11
Петр	5	3	3	12
Иван	6	3	3	13
Лиза	6	3	3	13

Часть A

1. Compute the Fourier expansions of the following functions.

   (a) The *selection function* $\mathrm{Sel} : \{-1,1\}^3 \to \{-1,1\}$ which outputs x_2 if $x_1 = -1$ and outputs x_3 if $x_1 = 1$.

   (b) The density function corresponding to the product probability distribution on $\{-1,1\}^n$ in which each coordinate has mean $\rho \in [-1,1]$;

   (c) The *hemi-icosahedron function* $\mathrm{HI} : \{-1,1\}^6 \to \{-1,1\}$, defined as follows: $\mathrm{HI}(x)$ is 1 if the number of 1's in x is 1, 2, or 6. $\mathrm{HI}(x)$ is -1 if the number of -1's in x is 1, 2, or 6. Otherwise, $\mathrm{HI}(x)$ is 1 if and only if one of the ten facets in the following diagram has all three of its vertices 1:

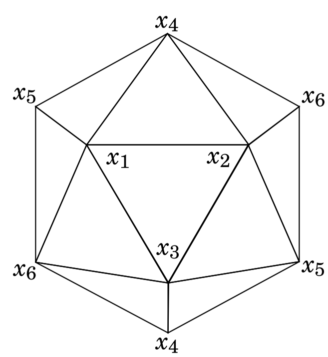

Рис. 1: The hemi-icosahedron

   (Please give some indication of how you arrived at the expansion; a bare formula does not suffice.)

2. Let $f : \{-1,1\}^n \to \{-1,1\}$.

   (a) Suppose $\mathbf{W}^1[f] = 1$. Show that $f(x) = \pm\chi_S$ for some $|S| = 1$.

   (b) Suppose $\mathbf{W}^{\leq 1}[f] = 1$. Show that f depends on at most 1 input coordinate.

(c) Suppose $\mathbf{W}^{\leq 2}[f] = 1$. Is it true that f depends on at most 2 input coordinates?

3. Let $A \subseteq \mathbb{F}_2^n$, let $\alpha = |A|/2^n$, and write $1_A : \mathbb{F}_2^n \to \{0,1\}$ for the indicator function of A.

   (a) Show that $\sum_{S \neq \emptyset} \widehat{1_A}(S)^2 = \alpha(1-\alpha)$.

   (b) Define $A + A + A = \{x + y + z : x, y, z \in A\}$, where the addition is in $\mathbb{F}_2^n$. Show that either $A + A + A = \mathbb{F}_2^n$ or else there exists $S^* \neq \emptyset$ such that $|\widehat{1_A}(S^*)| \geq \frac{\alpha}{1-\alpha} \cdot \alpha$. (Hint: if $A + A + A \neq \mathbb{F}_2^n$, show there exists $x \in \mathbb{F}_2^n$ such that $1_A * 1_A * 1_A(x) = 0$.)

4. For functions $f : \mathbb{F}_2^n \to \mathbb{R}$, sometimes it is more natural to index the Fourier coefficients not by subsets $S \subseteq [n]$ but by elements $\gamma \in \mathbb{F}_2^n$; here we identify a subset with its indicator vector. In this case we would write the Fourier expansion as

$$f = \sum_{\gamma \in \mathbb{F}_2^n} \widehat{f}(S)\chi_\gamma, \qquad \text{where } \chi_\gamma(x) = (-1)^{\gamma \cdot x}$$

   and $\gamma \cdot x$ is the dot-product of γ and x in the vector space $\mathbb{F}_2^n$. Note that for $\beta, \gamma \in \mathbb{F}_2^n$ we have $\chi_\beta \chi_\gamma = \chi_{\beta+\gamma}$.

   (a) Let H be a vector subspace of $\mathbb{F}_2^n$. Let $H^\perp$ be its "perpendicular subspace"; i.e., $H^\perp = \{\gamma \in \mathbb{F}_2^n : \gamma \cdot x = 0 \text{ for all } x \in H\}$. Show that the indicator function $1_H : \mathbb{F}_2^n \to \{0,1\}$ of H has the Fourier expansion $1_H = \sum_{\gamma \in H^\perp} 2^{-k} \chi_\gamma$, where $k = \dim(H^\perp)$. (Remark: $k = n - \dim(H)$ is sometimes denoted $\mathrm{codim}(H)$.)

   (b) Given the subspace H and also $y \in \mathbb{F}_2^n$, the set $H + y = \{h + y : h \in H\}$ is called an "affine subspace" of $\mathbb{F}_2^n$. Show that the indicator function $1_{H+y} : \mathbb{F}_2^n \to \{0,1\}$ of this affine subspace has the Fourier expansion $1_{H+y} = \sum_{\gamma \in H^\perp} 2^{-k} \chi_\gamma(y) \chi_\gamma$, where again $k = \dim(H^\perp)$.

5. In 1965, the Nassau County (New York) Board used a weighted majority voting system to make its decisions, with the 6 towns getting differing weights based on their population. Specifically, the board used the voting rule $f : \{0,1\}^6 \to \{-1,1\}$ defined by $f(x) = \mathrm{sgn}(-58 + 31x_1 + 31x_2 + 28x_3 + 21x_4 + 2x_5 + 2x_6)$. Compute $\mathbf{Inf}_i[f]$ for all $i \in [6]$. (PS: John Banzhaf invented the notion of $\mathbf{Inf}_i$ while suing on behalf of towns #5 and #6.)

6. Let $f : \{-1,1\}^n \to \{-1,1\}$ be unbiased (i.e., $\mathbf{E}[f] = 0$), and let $\mathbf{MaxInf}[f]$ denote $\max_{i \in [n]}\{\mathbf{Inf}_i[f]\}$.

   (a) Use the Poincare Inequality to show $\mathbf{MaxInf}[f] \geq 1/n$.

   (b) Prove $|\widehat{f}(i)| \leq \mathbf{Inf}_i[f]$ for all $i \in [n]$. (Hint: consider $\mathbf{E}[|\mathrm{D}_i f|]$.)

   (c) Prove that $\mathbf{I}[f] \geq 2 - n\mathbf{MaxInf}[f]^2$. (Hint: first prove $\mathbf{I}[f] \geq \mathbf{W}^1[f] + 2(1 - \mathbf{W}^1[f])$ and then use the previous exercise.)

   (d) Deduce that $\mathbf{MaxInf}[f] \geq \frac{2}{n} - \frac{4}{n^2}$.

7. In this exercise you are asked to prove some fancily-named properties of the noise operator T_ρ.

   (a) Show that T_ρ is "positivity-preserving" for all $\rho \in [-1,1]$, meaning $f \geq 0 \Rightarrow \mathrm{T}_\rho f \geq 0$. Show also that it is "positivity-improving" for all $\rho \in (-1,1)$, meaning $f \geq 0, f \not\equiv 0 \Rightarrow \mathrm{T}_\rho f > 0$.

   (b) Show the "semigroup property": $\mathrm{T}_{\rho_1} \circ \mathrm{T}_{\rho_2} = \mathrm{T}_{\rho_1 \rho_2}$ for all $\rho_1, \rho_2, \in [0,1]$. (If you like, prove it even for $\rho_1, \rho_2 \in [-1,1]$.)

(c) Show that T_ρ is a "contraction on L^p" for all $p \geq 1$ and $\rho \in [-1,1]$; i.e., $\|\mathrm{T}_\rho f\|_p \leq \|f\|_p$, where $\|f\|_p = \mathbf{E}_{\boldsymbol{x}}[|f(\boldsymbol{x})|^p]^{1/p}$.

8. Suppose the Fourier spectrum of $f : \{-1,1\}^n \to \mathbb{R}$ is ϵ_1-concentrated on $\mathcal{F}$ and that $g : \{-1,1\}^n \to \mathbb{R}$ satisfies $\|f-g\|_2^2 \leq \epsilon_2$. Show that the Fourier spectrum of g is $2(\epsilon_1+\epsilon_2)$-concentrated on $\mathcal{F}$.

9. (a) Let $k \in \mathbb{N}^+$ and let $\mathcal{C} = \{f : \{-1,1\}^n \to \{-1,1\} \mid \deg(f) \leq k\}$. (In particular, $\mathcal{C}$ contains all functions computable by depth-k decision trees.) Show that $\mathcal{C}$ is learnable from random examples with error 0 in time $n^k \cdot \mathrm{poly}(n, 2^k)$. You may use the following "Degree/Granularity Fact": for every $f \in \mathcal{C}$ and every $S \subseteq [n]$, the Fourier coefficient $\widehat{f}(S)$ is an integer multiple of 2^{1-k}.

   (b) Prove the Degree/Granularity Fact.

Часть B

10. Let $\mathcal{H} = \{f : [m] \to [l]\}$ be a pairwise independent hash family and let $l \geq n^2$. Then for any $S \subseteq [m]$ of size $|S| = n$, there exists an $h \in \mathcal{H}$ such that the restriction $h|_S$ is a one to one function from S to $[l]$.

11. Let k be a constant. Let $X \subseteq \{0,1\}^n$ with $|X| = o(n^{k/2})$. Show that for $d = \lfloor k/2 \rfloor$, there is a function $f : \{0,1\} \to \mathbb{R}$ which satisfies: 1) f is not identically 2) $\hat{f}(S) = 0$ for each $|S| > d$. 3) $f(x) = 0$ for each $x \in X$. Use this to show that any k-wise independent distribution over $\{0,1\}^n$ has support at least $\Omega(n^{k/2})$.

12. Show that for any ϵ-biased distribution μ, $\sum_{x\in\{0,1\}^n} \mu^2(x) \leq \epsilon^2 + \frac{1}{2^n}$. Conclude that if $\epsilon < 1/2^{n/2}$, then μ must have support at least $\frac{1}{2}2^n$.

13. Let μ be an ϵ-biased distribution on $\{0,1\}^n$. Let t be a parameter to be chosen later. Let $\nu = \mu * \mu * \cdots * \mu$ (t times). 1) Show that ν is an ϵ^t-biased distribution. 2) Show that $|Support(\nu)| \leq \binom{|Support(\mu)|+t}{t}$ 3) Combine these with the previous problem to show that $|Support(\mu)| = \Omega\left(\frac{n}{\epsilon^2 \log \frac{1}{\epsilon}}\right)$

14. Show a correspondence between ϵ-bias generators $G : \{0,1\}^k > 0, 1^{l(k)}$ and binary linear error-correcting codes $C : 0, 1^{l(k)} > 0, 1^{2^k}$ such that every two codewords are at distance $(1 \pm \epsilon(k))2^{k-1}$ apart. Guideline: Consider G such that the i-th bit of $G(j)$ equals the j-th bit of $C(0^{i-1}10^{l(k)-i})$.

Часть C

15. Оцените сверху вероятность того, что при случайном блуждании длины ℓ по (n,d,α)-экспандеру множество B плотности ρ будет посещено как минимум $\beta\ell$ раз.

16. Пусть H_n^m — семейство попарно независимых хеш-функций. Пусть $S \subseteq \{0,1\}^n$. Пусть случайная величина H распределена равномерно на H_n^m, а случайная величина X равномерно на S. Докажите, что статистическое расстояние между распределением, задаваемым случайной величиной $(H, H(X))$ и случайной величиной H, U_m не превосходит $\epsilon = (\frac{2^m}{|S|})^{\Omega(1)}$.

17. Определим функцию Ext : $\{0,1\}^n \times \{0,1\}^t \to \{0,1\}^n$, которая по коду вершины $(2^n, d, \frac{1}{2})$-алгебраического экспандера выдает код вершины после блуждания, которое закодировано в строке t. Покажите, что для каждого k и $\epsilon > 0$ существует $t = O(n - k + \log \frac{1}{\epsilon})$, что так определенная функция Ext является (k, ϵ)-экстрактором.

18. Пусть Ext : $\{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ — это (k, ϵ)-экстрактор. Покажите, что алгоритм, который получет случайную строку r длины n и делает 2^d запросов $\{\mathrm{Ext}(r,s) \mid s \in \{0,1\}^d\}$ к функции $f : \{0,1\}^m \to [0,1]$ и выдает среднее арифмитическое полученных ответов, является усредняющим сэмплером с точностью ϵ и ошибкой $\delta = 2^{-(n-k-1)}$.

19. Покажите, что существуют эффективные хиттеры с следующими параметрами: а) $q = \frac{1}{\epsilon} \log \frac{1}{\delta}$ и $r = \frac{n}{\epsilon} \log \frac{1}{\delta}$. б) $q = \frac{1}{\epsilon\delta}$ и $r = 2n$; в) $q = O(\frac{1}{\epsilon} \log \frac{1}{\delta})$ и $r = 2n + O(\log \frac{1}{\delta})$. ($\delta$ — это вероятность неудачи, а ϵ — это доля единиц функции f).