Г. И. Ивченко, Ю. И. Медведев (Москва, МИЭМ). **Вопросы анализа спектра случайной булевой функции.**

1. Пусть V_n — n-мерное линейное пространство над полем из двух элементов, $f = f(x)$ $(x \in V_n)$ — булева функция от n переменных, $\operatorname{Im}_n = \{f\}$ — множество всех булевых функций на V_n. Для двух векторов $\overline{x} = (x_1, \ldots, x_n)$, $\overline{y} = (y_1, \ldots, y_n)$ скалярное произведение в V_n есть $(x, y) = \sum_{i=1}^{n} \oplus x_i y_i$ (символ $\oplus$ означает суммирование по модулю 2); $\|f\|$ означает вес функции f.

Величину $\Delta_{\overline{\alpha}}^{f} = \|f(x) \oplus (\overline{\alpha}, x)\| - 2^{n-1}$, $\overline{\alpha} \in V_n$, назовем *спектральным коэффициентом функции* f, отвечающим вектору α, а совокупность этих величин по всей совокупности $\alpha \in V_n$ назовем *спектром функции* f: $\overline{\Delta}^{f} = \{\Delta_{\overline{\alpha}}^{f},\ \alpha \in V_n\}$. Они однозначно определяют функцию f.

Введем на множестве Im_n равномерную меру, приписывающую каждой функции $f \in \operatorname{Im}_n$ вес 2^{2^n}. Тогда спектр $\overline{\Delta}^{f}$ становится случайным вектором размерности 2^n.

Актуальные задачи, стоящие перед специалистами в этой области, — исследовать распределения (как точные, так и асимптотические при $n \to \infty$) различных характеристик спектра $\overline{\Delta}^{f}$ в случаях, когда задается равномерная мера как на всем множестве Im_n, так и на различных подмножествах Im_n. Литература, относящаяся к этой тематике, огромна (работы О. В. Денисова, О. А. Логачева, Б. В. Рязанова, А. А. Сальникова, Ю. В. Тараннikова, А. В. Черемушкина, С. И. Чечеты и др.).

Известно, что для решения задач такого типа при исследовании случайных подстановок и других комбинаторных структур большую роль играет такой аналитический аппарат, как производящие (характеристические) функции указанных объектов. Наша цель в этой заметке — найти производящую функцию спектра случайной двоичной функции и получить отдельные результаты анализа $\overline{\Delta}^{f}$ при помощи этого аппарата.

2. Обозначим $N_n(\Delta)$ число булевых функций $f \in \operatorname{Im}_n$, имеющих спектр $\overline{\Delta}$. Оно равно 0 или 1. Производящую функцию (пр. ф.) F_n этих величин обозначим $F_n(z_0, z_1, \ldots, z_{2^n-1}) = \mathbf{E}\, \overline{z}^{\overline{\Delta}} = \sum_{\overline{\Delta}} N_n(\overline{\Delta}) \prod_{j=0}^{2^n-1} z_j^{\Delta_j}$.

Введем более удобную для наших целей нумерацию векторов $\overline{\alpha}$, $\overline{\Delta}$. Обозначим $\overline{\alpha}_{i_1 \ldots i_k}$ вектор $\overline{\alpha} \in V_n$, имеющий k единиц, стоящих на местах $1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n$, а остальные $n-k$ координат равны 0; в частности, $\overline{\alpha}_0 = (0, \ldots, 0)$, $\overline{\alpha}_1 = (0, \ldots, 0, 1)$, $\ldots$, $\overline{\alpha}_{12\ldots n} = (1, \ldots, 1)$. Соответствующим образом занумеруем спектральные коэффициенты $\Delta_{i_1 \ldots i_k}^{f}$ и переменные $z_{i_1 \ldots i_k}$ в пр. ф. $F_n(\overline{z})$.

Наконец, введем ключевую для дальнейшего изложения функцию $U(z) = \sqrt{z} + 1/\sqrt{z}$. В этих обозначениях можно доказать, что общая производящая функция случайного спектра $\overline{\Delta}^{f}$ есть

$$\varphi_n(\overline{z}) = 2^{-2^n} F_n(\overline{z}) = \prod_{\substack{\beta = (\beta_1, \ldots, \beta_n) \\ \beta_0 = \pm 1}} \left(\frac{1}{2} U\left(z_0 \prod_{\substack{1 \leqslant i_1 < \cdots < i_k \leqslant n \\ k = 1, \ldots, n}} z_{i_1 \ldots i_k}^{\beta_{i_1 \ldots i_k}} \right) \right).$$

3. Несмотря на кажущуюся громоздкость формулы, она дает возможность решать интересные задачи, связанные со случайным спектром. Производящие функции для подмножеств F_n' и F_n'' функций с четными и нечетными весами с соответственно равномерными мерами на них равны:

$$\varphi_n'(z_0, z_1, \ldots, z_{2^n-1}) = \frac{1}{2}\Big[\varphi_n(z_0, z_1, \ldots, z_{2^n-1}) - \varphi_n(-z_0, z_1, \ldots, z^{2^n-1})\Big],$$

$$\varphi_n''(z_0, z_1, \ldots, z_{2^n-1}) = \frac{1}{2}\Big[\varphi_n(z_0, z_1, \ldots, z_{2^n-1}) + \varphi_n(-z_0, z_1, \ldots, z^{2^n-1})\Big].$$

Коэффициенты разложения $\varphi_n(\overline{z})$ по степеням z_0

$$\varphi_n(\overline{z}) = \sum_{k=-2^{n-1}}^{2^{n-1}} z_0^k V_k(z_1, \ldots, z_{2^n-1})$$

обладают следующими свойствами:

$$V_{-k}(z_1, \ldots, z_{2^n-1}) = V_k(z_1^{-1}, \ldots, z_{2^n-1}^{-1}), \quad k = 0, 1, \ldots, 2^{n-1}, \quad V_{-2^{n-1}} = V_{2^n-1} = 1;$$

$V_{|k|}$ имеет $C_{2^n}^k$ слагаемых; если $|k|$ — четное (нечетное), то все переменные входят в слагаемые четной (нечетной) степени, $V_0(z_1, \ldots, z^{2^n-1})$ соответствуют производящей функции для множества равновероятных функций.

4. Положив какие-либо z_i равными единице, получим производящие функции для интересующих нас подвекторов $\overline{\Delta}$. На этом пути можно получить как известные в настоящее время результаты, так и неизвестные. Ограничимся рассмотрением простейшего случая распределения двумерных векторов (Δ_i, Δ_j), i, j — произвольные:

$$\mathbf{E}\, z_i^{\Delta_i} z_j^{\Delta_j} = (z_i z_j)^{-2^{n-1}} \left[\frac{(z_i + z_j)(1 + z_j z_j)}{4}\right]^{2^{n-1}}.$$

Отсюда получаем

$$\mathbf{P}\{\Delta_i = l,\ \Delta_j = s\} = \binom{2^{n-1}}{2^{n-2} + (l+s)/2} \binom{2^{n-1}}{2^{n-2} + (l-s)/2} 2^{-2^n},$$

и условное распределение

$$\mathbf{P}\left\{\Delta_i + 2^{n-1} = \frac{l+M}{2} \,\middle|\, \Delta_j + 2^{n-1} = l\right\} = \binom{2^{n-1}}{(l+m)/2} \binom{2^{n-1}}{(l-m)/2} \Big/ \binom{2^n}{l}, \quad 0 \leqslant l, m \leqslant 2^n.$$

Это гипергеометрическое распределение. В качестве предельных при $n \to \infty$, очевидно, получим биномиальное распределение (при конечном l) и нормальное распределение (при $l, m \to \infty$ так, что $l/2^n \to t$, $0 < t < 1$, и $m 2^{n/2-2} \sqrt{t(1-t)} \to x$, x — конечное число).

Первые моменты элементов спектра имеют следующий вид:

$$\mathbf{E}\,\Delta_i = 0, \quad \mathbf{D}\,\Delta_i = 2^{n-2}, \quad \operatorname{cov}(\Delta_i, \Delta_j) = 0, \quad i \neq j, \quad \mathbf{E}\,(\Delta_i \Delta_j \Delta_k) = -2^{n-4}.$$

5. Анализ интересующих нас подвекторов спектра $\overline{\Delta}^f$ можно проводить с использованием линейных преобразований компонент. Так, асимптотическая нормальность подвекторов при $n \to \infty$ следует из соотношения $\overline{\Delta}^f = 0,5 H_{2^n} \overline{\zeta}$, где вектор $\overline{\zeta}$ состоит из независимых компонент, имеющих сдвинутое биномиальное распределение, а $H_{2^n} = ((-1)^{(\alpha_i, \alpha_j)})$ $(i, j = 0, 1, \ldots, 2^n - 1)$ — матрица Адамара–Сильвитра. Стало быть, это — ортогональное преобразование, сохраняющее свойство нормальности распределений (от $\overline{\zeta}$ к $\overline{\Delta}$).