В. А. Копытцев, **В. Г. Михайлов** (Москва, АК РФ, МИАН).
Об одном асимптотическом свойстве сфер в дискретных простанствах большой размерности.

В связи с исследованием асимптотических свойств распределения числа решений случайных линейных включений над конечных полем K возникает задача изучения свойства последовательностей множеств в векторных пространствах V^m над K растущей размерности m, названного авторами «асимптотической свободой множества от линейных комбинаций его элементов» (примеры использования этого понятия можно найти в работах [1–3]). Опишем это свойство.

Пусть m — натуральное число, $N(a_1, a_2, a_3, c, H)$ — число решений системы из m линейных уравнений над полем K, записанной в виде уравнения $a_1u^1 \oplus a_2u^2 \oplus a_3u^3 = c$, относительно тройки векторов $(u^1, u^2, u^3) \in H^3$, где H — некоторое заданное подмножество V^m, $a_1, a_2, a_3 \in K\backslash\{0\}$, $c \in V^m$. Знак $\oplus$ обозначает сложение векторов в линейных пространствах над полем K. Положим $N(H) = \max_{a_1,a_2,a_3,c} N(a_1, a_2, a_3, c, H)$, $\rho(H) = N(H)/|H|^2$, где $|H|$ обозначает число элементов конечного множества B. Нетрудно проверить, что $|H|^{-1} \leqslant \rho(H) \leqslant 1$.

Отношение $\rho(H) = N(H)/|H|^2$ является своего рода мерой отличия множества H от линейного или аффинного пространства. Для линейных и аффинных подпространств эта мера принимает максимально возможное значение $\rho(H) = 1$.

Пусть $H = H(m) \subset V^m$ и $m \to \infty$. Тогда условие $\rho(H) \to 0$ можно трактовать как «асимптотическую свободу» (при $m \to \infty$) множества $H = H(m)$ от линейных комбинаций его элементов.

В докладе рассматриваются последовательности шаров и сфер (в метрике Хемминга): $S_r(y^0) = \{y \in V^m\colon 1 \leqslant \|y-y^0\| \leqslant r(m)\}$, $S'_r(y^0) = \{y \in V^m\colon \|y-y^0\| = r(m)\}$. Здесь $\|x\|$ — число ненулевых элементов в записи вектора $x \in V^m$. Отметим, что значения функции ρ на шарах и сферах не зависят от выбора их центра y^0: $\rho(S_r(y^0)) = \rho(S_r(0^m))$, $\rho(S'_r(y^0)) = \rho(S'_r(0^m))$.

В работе [1] было доказано следующее утверждение.

Теорема 1. *Если $m \to \infty$, $r = r(m) \geqslant 1$, $r(m)/m \leqslant \rho$ при некотором числе $0 < \rho < (q-1)/q$, то $\rho(S_r(y^0)) \to 0$ и $\rho(S'_r(y^0)) \to 0$ при любых $y^0 = y^0(m) \in V^m$.*

Основной результат доклада касается свойств сфер и состоит в следующем.

Теорема 2. *Пусть $K = \mathrm{GF}(q)$, $m \to \infty$, $1 \leqslant r = r(m) \leqslant m-1$, если $q = 2$, $1 \leqslant r = r(m) \leqslant m$, если $q \geqslant 3$. Тогда $\rho(S'_r(y^0)) \to 0$ при любых $y^0 = y^0(m) \in V^m$.*

Таким образом, сферы обладают свойством «асимптотической свободы от линейных комбинаций» (с ростом размерности пространства) при любом изменении их радиуса, обеспечивающем неограниченный рост числа элементов сферы.

СПИСОК ЛИТЕРАТУРЫ

1. *Копытцев В. А.*, *Михайлов В. Г.* Теоремы пуассоновского типа для числа специальных решений случайного линейного включения. — Дискретн. матем., 2010, т. 22, в. 2, с. 3–21.
2. *Копытцев В. А.*, *Михайлов В. Г.* Теоремы пуассоновского типа для числа решений случайных включений. — Математические вопросы криптографии, 2010, т. 1, в. 4, с. 63–84.
3. *Копытцев В. А.*, *Михайлов В. Г.* О распределении чисел решений случайных включений. — Математические вопросы криптографии, 2011, т. 2, в. 2, с. 81–107.