**Theorem 6.** *Let $t$ and $u$ be natural numbers with $0 \leq t < u$ and let $A$ be a proper non-empty subset of the vector space $\mathbb{Z}_2^u$. Set $\alpha = 1 - \frac{|A|}{2^u}$. Then for a random uniformly chosen surjective linear mapping $T : \mathbb{Z}_2^u \to \mathbb{Z}_2^t$ we have*

$$\mathbf{P}(T(A) \neq \mathbb{Z}_2^t) \leq \alpha^{u-t-\log t+\log\log \frac{1}{\alpha}}.$$

*Proof.* Set $s = u - t$. Choose vectors $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_s$ independently and randomly according uniform distribution. Let $\mathcal{T}$ be a set of all surjective linear mappings $T : \mathbb{Z}_2^u \to \mathbb{Z}_2^t$ with $T(\vec{v}_i) = \vec{0}$ for all $i = 1, 2, \ldots, s$. Then $T$ is a random uniformly chosen linear surjective mapping from $\mathbb{Z}_2^u$ onto $\mathbb{Z}_2^t$. The set $\{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_s\}$ of vectors need not be linearly independent. Let us define $A_0 = A$ and $A_i = A_{i-1} \cup (A_{i-1} + \vec{v}_i)$ and set $\alpha_i = 1 - \frac{|A_i|}{2^u}$. If we consider that $\alpha_i$ is a random variable then, by Lemma 2, $\mathbf{E}(\alpha_i) = \alpha_{i-1}^2$ for all $i = 1, 2, \ldots, s$. Then $0 < \alpha_0 < 1$ and clearly $\alpha_i \leq \alpha_{i-1}$ for all $i = 1, 2, \ldots, s$. Thus the assumptions of Lemma 3 are fulfilled and, by Lemma 3,

$$\begin{aligned}\mathbf{P}(\alpha_s \geq 2^{-t}) \leq & \alpha^{s-\log\log(\frac{1}{2^{-t}})+\log\log(\frac{1}{\alpha})} = \\ & \alpha^{s-\log t+\log\log(\frac{1}{\alpha})} = \alpha^{u-t-\log t+\log\log(\frac{1}{\alpha})}.\end{aligned}$$

Since $\alpha_s = 1 - \frac{|A_s|}{2^u}$ we infer that $|A_s| = 2^u(1 - \alpha_s)$ and hence from $\alpha_s < 2^{-t}$ it follows that $|A_s| > 2^u - 2^{u-t}$. Since kernel of $T$ has a size $2^{u-t}$ we infer that $T(A_s) = T(\mathbb{Z}_2^u)$ and hence $T(A_s) = \mathbb{Z}_2^t$ because $T$ is surjective. Thus

$$\mathbf{P}(\alpha_s < 2^{-t}) = \mathbf{P}(T(A_s) = \mathbb{Z}_2^t).$$

Since $\mathbb{Z}_2^u$ is a vector space over a field $\mathbb{Z}_2$ we obtain, by induction over $i$ that $A_i = A + \mathrm{spam}(\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_s)$. Since $T(\vec{v}_i) = \vec{0}$ for all $i = 1, 2, \ldots, i$ we state that $T(A) = T(A_i)$ for all $i = 1, 2, \ldots, s$. Hence

$$\mathbf{P}(T(A) \neq \mathbb{Z}_2^t) = \mathbf{P}(T(A_s) \neq \mathbb{Z}_2^t) = \mathbf{P}(\alpha_s \geq 2^{-t}) \leq \alpha^{u-t-\log t+\log\log(\frac{1}{\alpha})}$$

and the proof follows. $\square$

Typeset by $\mathcal{AMS}$-TEX