Theorem. *Let u and t be non-zero natural numbers and let p be a prime. Then the family of all linear mappings from $\mathbb{Z}_p^u$ into $\mathbb{Z}_p^t$ is 1-universal.*

Proof. Let $A = \{\vec{a}_1, \vec{a}_2, \dots, \vec{a}_u\}$ be a base of $\mathbb{Z}_p^u$. It is well known that for every mapping $f : A \longrightarrow \mathbb{Z}_p^t$ there exists a unique linear mapping extended f and $|\mathbb{Z}_p^t| = p^t$. Thus the number of linear mapping from $\mathbb{Z}_p^u$ into $\mathbb{Z}_u^t$ is $(p^t)^u = p^{tu}$. Let $\vec{x}$ and $\vec{y}$ be distinct vectors of $\mathbb{Z}_p^u$ and let $j \in \{1, 2, \dots, u\}$ such that if $\vec{x} - \vec{y} = \sum_{i=1}^n b_i \vec{a}_i$ then $b_j \neq 0$ (since $\vec{0} \neq \vec{x} - \vec{y}$ such j exists). Then $f : \mathbb{Z}_p^u \longrightarrow \mathbb{Z}_p^t$ is a linear mapping with $f(x) = f(y)$ if and only if $f(\vec{x} - \vec{y}) = f(\vec{x}) - f(\vec{y}) = \vec{0}$. Thus for every mapping $g : A \setminus \{a_j\} \longrightarrow \mathbb{Z}_p^t$ there exists exactly one linear mapping $f : \mathbb{Z}_p^u \longrightarrow \mathbb{Z}_p^t$ with $f(x) = f(y)$ because necessarily

$$f(\vec{a}_j) = \sum_{i=1, i \neq j}^{i} b_i g(\vec{a}_i).$$

Hence the number of linear mappings $f : \mathbb{Z}_p^u \longrightarrow \mathbb{Z}_p^t$ with $f(\vec{x}) = f(\vec{y})$ is equal to $(p^t)^{u-1} = p^{t(u-1)}$. From $p^{t(u-1)} = \frac{p^{tu}}{p^t}$ it follows that the family of all linear mappings from $\mathbb{Z}_p^u$ into $\mathbb{Z}_p^T$ is 1-universal. $\square$

Theorem 3. *For every ε with $0 < \varepsilon < 1$ there exists a constant $c_\varepsilon > 0$ such that for all natural numbers w and t and for every set $A \subseteq \mathbb{Z}_2^w$ with $|A| \geq c_\varepsilon t 2^t$ we have*

$$\mathbf{P}(T(A) = \mathbb{Z}_2^t) \geq 1 - \varepsilon$$

for every random uniformly chosen linear mapping $T : \mathbb{Z}_2^w \longrightarrow \mathbb{Z}_2^t$.

Proof. Set $u = \lceil \log(\frac{2|A|}{\varepsilon}) \rceil$. Let $T_1 : \mathbb{Z}_2^u \longrightarrow \mathbb{Z}_2^t$ be a random uniformly chosen surjective linear mapping (since $u \geq t$ such mapping exists). Fix T_1. Then for every random uniformly chosen linear mapping $T : \mathbb{Z}_2^w \longrightarrow \mathbb{Z}_2^t$ there exists a linear mapping $T_0 : \mathbb{Z}_2^w \longrightarrow \mathbb{Z}_2^u$ with $T = T_0 \circ T_1$ and T_0 is a random linear mapping with uniform distribution. Since the family of all linear mappings from $\mathbb{Z}_2^w$ into $\mathbb{Z}_2^u$ is 1-universal we conclude that

$$\mathbf{P}(T_0(\vec{x}) = T_0(\vec{y})) = 2^{-u}$$

for all distinct vectors $\vec{x}$ and $\vec{y}$ from $\mathbb{Z}_2^w$. If d_A is the number of all pairs of distinct vectors $\vec{x}, \vec{y} \in A$ with $T_0(\vec{x}) = T_0(\vec{y})$ then the expected value of a random variable d_A is

$$\mathbf{E}(d_A) = \binom{|A|}{2} 2^{-u}.$$

If $|T_0(A)| \leq \frac{|A|}{2}$ then there exist at least $\frac{|A|}{2}$ pairs of distinct vectors $\vec{x}, \vec{y} \in A$ with $T_0(\vec{x}) = T_0(\vec{y})$. By Markov inequality

$$\mathbf{P}(c_A \geq k \binom{|A|}{2} 2^{-u}) \leq \frac{1}{k}.$$

Typeset by $\mathcal{AMS}$-TEX

Thus if we set $k = \frac{|A|2^u}{2\binom{|A|}{2}}$ then we obtain

$$\mathbf{P}(|T_0(A)| \geq \frac{|A|}{2}) \leq \mathbf{P}(d_A \geq \frac{|A|}{2}) \leq \frac{2\binom{|A|}{2}}{|A|2^u} = \frac{|A|-1}{2^u} < \frac{|A|}{2^u} \leq \frac{\varepsilon|A|}{2|A|} = \frac{\varepsilon}{2}$$

We can summarize that

$$\mathbf{P}(T(A) \neq \mathbb{Z}_2^t \wedge |T_0(A)| \leq \frac{|A|}{2}) \leq \frac{\varepsilon}{2}.$$

Secondly we compute $\mathbf{P}(T(A) \neq \mathbb{Z}_2^t \wedge |T_0(A)| \geq \frac{|A|}{2})$. By Theorem 6 for $T_1 : \mathbb{Z}_2^u \longrightarrow \mathbb{Z}_2^t$ and $T_0(A) \subseteq \mathbb{Z}_2^u$, we have

$$\mathbf{P}(T(A) = T_1(T_0(A)) \neq \mathbb{Z}_2^t \wedge |T_0(A)| \geq \frac{|A|}{2}) \leq \alpha^{u-t-\log t+\log\log(\frac{1}{\alpha})}$$

where $\alpha = 1 - \frac{|T_0(A)|}{2^u}$. Clearly

$$\alpha < 1 - \frac{|A|}{2}2^{-\log(\frac{2|A|}{\varepsilon})-1} = 1 - \frac{|A|}{4\frac{2|A|}{\varepsilon}} = 1 - \frac{\varepsilon}{8} \leq e^{-\frac{\varepsilon}{8}}.$$

Set $c_\varepsilon = 4(\frac{2}{\varepsilon})^{\frac{8}{\varepsilon}}$. Then we can estimate

$$\begin{aligned}
-\frac{\varepsilon}{8}(u - t - \log t + \log\log(\frac{1}{\alpha})) &= -\frac{\varepsilon}{8}(\lceil\log(\frac{2|A|}{\varepsilon})\rceil - t - \log t + \log\log(\frac{1}{\alpha})) = \\
&-\frac{\varepsilon}{8}(\lceil\log(\frac{8(\frac{2}{\varepsilon})^{\frac{8}{\varepsilon}}t2^t}{\varepsilon})\rceil - t - \log t + \log\log(\frac{1}{\alpha})) \leq \\
&-\frac{\varepsilon}{8}(3 + \frac{8}{\varepsilon}\log\frac{2}{\varepsilon} - \log\varepsilon + \log t + t - t - \log t + \log(\frac{\varepsilon}{8}\log e)) = \\
&-\frac{\varepsilon}{8}(3 - \log\varepsilon + \frac{8}{\varepsilon}\log(\frac{2}{\varepsilon}) + \log\varepsilon - 3 + \log\log e) = \\
&-\frac{\varepsilon}{8}(\frac{8}{\varepsilon}\log(\frac{2}{\varepsilon}) + \log\log e) = \\
&\log\frac{\varepsilon}{2} - \frac{\varepsilon}{8}\log\log e \leq \log\frac{\varepsilon}{2}.
\end{aligned}$$

Hence we infer that

$$\begin{aligned}
\mathbf{P}(T(A) = T_1(T_0(A)) \neq \mathbb{Z}_2^t \wedge |T_0(A)| \geq \frac{|A|}{2}) \leq &\alpha^{u-t-\log t+\log\log(\frac{1}{\alpha})} \leq \\
&e^{-\frac{\varepsilon}{8}(u-t-\log t+\log\log(\frac{1}{\alpha}))} \leq \\
&e^{\log(\frac{\varepsilon}{2})} \leq e^{\ln(\frac{\varepsilon}{2})} = \frac{\varepsilon}{2}.
\end{aligned}$$

If we connect both alternatives we deduce that

$$\mathbf{P}(T(A) = T_1(T_0(A)) \neq \mathbb{Z}_2^t) \leq \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$$

and form this it follows that $\mathbf{P}(T(A) = \mathbb{Z}_2^t) \geq 1 - \varepsilon$. $\square$