Polynomial Differences and Sárközy's Theorem

Bogdan Grechuk · 2 Nov 2026

https://functor.network/user/3333/entry/2045

In October 2026, OpenAI released a preprint (OpenAI 2026a) announcing a substantial strengthening of a classical theorem in combinatorial number theory. The result concerns a simple question: how large can a set of integers be if no two of its elements differ by a value of a given polynomial?

Let us begin with an example. Suppose that A is a subset of

$$\{1, 2, \dots, N\}$$

such that the difference between any two distinct elements of A is never a perfect square. For example, the set $A = \{1, 3, 8\}$ has this property, since its positive differences are 2, 5, and 7.

How large can such a set be?

In 1978, Sárkőzy (Sárközy 1978) proved that

$$\lim_{N \to \infty} \frac{r(N)}{N} = 0,$$

where $r(N)$ is the maximum possible size of a subset $A \subseteq \{1, \dots, N\}$ without two distinct elements whose difference is a perfect square.

Thus, such sets must become increasingly sparse. More precisely, their proportion among the integers from 1 to N tends to zero as $N \to \infty$.

This result is closely related to Szemerédi's theorem, which states that every subset of the positive integers with positive upper density contains arbitrarily long arithmetic progressions. We discussed a related quantitative problem in an earlier post.

However, Sárkőzy's theorem concerns differences of the special form n^2, rather than ordinary arithmetic progressions. A natural generalization asks what happens if squares are replaced by the values of an arbitrary polynomial.

Let

$$h(x) = a_k x^k + \cdots + a_1 x + a_0$$

be a polynomial with integer coefficients and degree $k \geq 2$, so that $a_k \neq 0$.

We would like to know how large a set A can be if the equation

$$a - b = h(n)$$

has no solutions with $a, b \in A$, $a \neq b$, and n a positive integer.

There is an obvious obstruction. For example, consider

$$h(x) = x^2 + 1.$$

This polynomial is never divisible by 3, because every square is congruent to 0 or 1 modulo 3. Consequently, the set

$$A = \{3, 6, 9, \ldots, 3\lfloor N/3 \rfloor\}$$

contains no two elements whose difference equals $h(n)$, although A contains approximately $N/3$ elements.

To exclude such examples, mathematicians introduce the following condition.

A polynomial h with integer coefficients is called *intersective* if, for every positive integer q, there exists an integer n such that

$$h(n) \equiv 0 \pmod{q}.$$

In other words, the polynomial has a root modulo every positive integer.

For example, $h(x) = x^2$ is intersective, and so is $h(x) = x(x+1)$. More interestingly, there exist intersective polynomials that have no integer roots at all.

In 1978, Kamae and Mendès France (Kamae and Mendès France 1978) generalized Sárkőzy's qualitative result to all nonconstant intersective polynomials. They proved that a subset of the positive integers with positive upper density must contain two distinct elements whose difference is a value of h.

But how quickly must the density of a set avoiding such differences tend to zero?

This quantitative question remained very difficult. Even for squares, the best bounds improved only gradually. In 2025, Green and Sawhney (Green and Sawhney 2025) established

$$r(N) \leq N \exp(-c\sqrt{\log N})$$

for some constant $c > 0$, where $\log$ denotes the natural logarithm.

A much stronger estimate would have the form

$$r(N) \leq C N^{1-\epsilon}$$

for some constants $C, \epsilon > 0$. Such an estimate is called a *power saving*, because it improves the trivial bound $r(N) \leq N$ by a fixed positive power of N.

In September 2026, OpenAI (OpenAI 2026b) posted a preprint claiming the first power-saving bound for sets without square differences.

The subsequent October 2026 preprint (OpenAI 2026a) extends this to all intersective polynomials, with an additional uniformity property.

Theorem 1 (OpenAI) *For every integer $k \geq 2$, there exists a constant $c_k > 0$ with the following property.*
Let h be any intersective polynomial of degree k with integer coefficients and positive leading coefficient. Then there exists a constant $C_h > 0$ such that every set

$$A \subseteq \{1, 2, \dots, N\}$$

satisfying

$$(A - A) \cap \{h(n) : n \geq 1\} \subseteq \{0\}$$

obeys

$$|A| \leq C_h N^{1-c_k}.$$

Here $A - A = \{a - b : a, b \in A\}$, and $|A|$ denotes the number of elements of A.
Thus, if a subset of $\{1, \dots, N\}$ contains more than $C_h N^{1-c_k}$ elements, then it must contain two distinct elements whose difference is a value of h at some positive integer.

The important feature of the theorem is that the exponent c_k depends *only on the degree k*, not on the coefficients of the polynomial. For example, all intersective quadratic polynomials with positive leading coefficient admit the same power-saving exponent, although the multiplicative constant C_h may vary.

Let us briefly discuss the proof. The authors build on the methods developed for the square-difference problem. A central ingredient is a carefully constructed collection of averages involving several variables, together with inequalities derived from repeated applications of the Cauchy–Schwarz inequality.

The difficulty in extending the argument from squares to general polynomials is that polynomial values behave differently when we restrict the integers to an arithmetic progression. The authors construct auxiliary polynomials that preserve the relevant difference patterns under such restrictions. They also develop Fourier-analytic estimates that control the distribution of polynomial values.

The main argument establishes an upper bound for certain averages that decreases by a fixed power of N whenever the set avoids the prescribed differences. On the other hand, these averages are bounded below by a positive

power of the density $|A|/N$. Comparing the two bounds gives the theorem. A careful normalization of the polynomial ensures that the final exponent depends only on its degree.

The result is a striking quantitative strengthening of the classical Furstenberg–Sárkőzy phenomenon. It tells us that, for every fixed intersective polynomial of degree at least two, a set avoiding all its nonzero values as differences must be polynomially smaller than the interval containing it.

The work is currently available as a preprint, and its proof awaits independent scrutiny. If confirmed, it will represent a major advance in understanding how polynomial patterns are forced to appear in sufficiently large sets of integers.

References

Green, Ben, and Mehtaab Sawhney. 2025. *New Bounds for the Furstenberg–Sárközy Theorem*. https://arxiv.org/abs/2411.17448.

Kamae, Tetsuya, and Michel Mendès France. 1978. “Van der Corput’s Difference Theorem.” *Israel Journal of Mathematics* 31 (3–4): 335–42. https://doi.org/10.1007/BF02761498.

OpenAI. 2026a. *A Power Saving for Intersective Polynomial Differences with an Exponent Depending Only on the Degree*. OpenAI Math Release preprint. https://github.com/openai/math/blob/main/preprints/A-power-saving-for-intersective-polynomial-differences-with-an-exponent-depending-only-on-the-degree-October-5-2026/power-saving-intersective-polynomial-differences.pdf.

OpenAI. 2026b. *A Power Saving for Square-Difference-Free Sets*. OpenAI Math Release preprint. https://github.com/openai/math/blob/main/preprints/A-power-saving-for-square-difference-free-sets-September-24-2026/paper.pdf.

Sárközy, András. 1978. “On Difference Sets of Sequences of Integers. I.” *Acta Mathematica Academiae Scientiarum Hungaricae* 31 (1–2): 125–49. https://doi.org/10.1007/BF01896079.