

APPROXIMATE HOMOMORPHISMS BETWEEN THE BOOLEAN CUBE AND GROUPS OF PRIME ORDER

TOM SANDERS

The purpose of this note is to highlight a question raised by Shachar Lovett [Lov], and to offer some motivation for its study. Our interest is in the existence of injections $f : (\mathbb{Z}/2\mathbb{Z})^n \rightarrow \mathbb{Z}/p\mathbb{Z}$ (where p is an odd prime) that are ‘approximately homomorphisms’ in the sense that $f(x + y) = f(x) + f(y)$ for many x and y . Lovett noted that if $p > 2^n$ then the map $f : (\mathbb{Z}/2\mathbb{Z})^n \rightarrow \mathbb{Z}/p\mathbb{Z}$ that ‘embeds in binary’ is an injection with¹

$$\mathbb{P}(f(x + y) = f(x) + f(y)) = \left(\frac{3}{4}\right)^n,$$

where x and y are taken uniformly and independently from $(\mathbb{Z}/2\mathbb{Z})^n$. We shall show the following complementary result.

Proposition 1.1. *Suppose that $f : (\mathbb{Z}/2\mathbb{Z})^n \rightarrow \mathbb{Z}/p\mathbb{Z}$ is an injection. Then*

$$\mathbb{P}(f(x + y) = f(x) + f(y)) = O\left(2^{-\frac{n}{11}}\right).$$

The method we use does generalise to other Abelian groups (see Theorem 1.3 below), but the next proposition captures perhaps the most interesting consequence. If G is a finite Abelian group then the structure theorem tells us there is a unique sequence of natural numbers $1 < d_1 \mid d_2 \mid \dots \mid d_n$ such that $G \cong (\mathbb{Z}/d_1\mathbb{Z}) \oplus \dots \oplus (\mathbb{Z}/d_n\mathbb{Z})$, and we say that G has n invariant factors.

Proposition 1.2. *Suppose that G and H are finite Abelian groups of co-prime order; G has n invariant factors; and $f : G \rightarrow H$ is an injection. Then*

$$\mathbb{P}(f(x + y) = f(x) + f(y)) = O\left(17^{-\frac{n}{79}}\right).$$

For comparison, $2^{-\frac{1}{11}} = 0.939\dots < 17^{-\frac{1}{79}} = 0.964\dots < 2^{-\frac{1}{20}}$.

We have presented Proposition 1.2 because it makes essential use of a result of Bukh [Buk08, Theorem 3] (formulated for quantitative reasons in the relevant special case in Lemma 2.1 below), without which the constant $17^{-\frac{1}{79}}$ would not be absolute². Indeed,

¹The map is defined by $f : (\mathbb{Z}/2\mathbb{Z})^n \rightarrow \mathbb{Z}/p\mathbb{Z}; (x_1, \dots, x_n) \mapsto x_1 + 2x_2 + \dots + 2^{n-1}x_n$, and the probability that $f(x + y) = f(x) + f(y)$ is the probability that we do not need to make a carry when adding $f(x)$ and $f(y)$. Indeed, $f(x) + f(y) - f(x + y) = 2x_1y_1 + 4x_2y_2 + \dots + 2^n x_n y_n$. Since 2 is invertible in $\mathbb{Z}/p\mathbb{Z}$ we can divide and then the right hand side is between 0 and $2^n - 1$. It follows that it equals 0 if and only if $x_i y_i = 0$ for all $1 \leq i \leq n$ from which the equality follows.

²As a concrete example, without Bukh’s result our arguments would give no information when $G = (\mathbb{Z}/p_n\mathbb{Z})^n$ where p_n is the n th prime.

Bukh's work raises a number of questions *e.g.* [Buk08, Question 16] around sunset inequalities, that bear on the problems of this paper.

We now state our main result for which we require a little more notation. Given an Abelian group G and $r \in \mathbb{Z}$ we write $K_{G,r}$ for the kernel of the homomorphism $G \rightarrow G; x \mapsto rx$, and given $A \subset G$ write $r \cdot A := \{ra : a \in A\}$.

Our main result is the following.

Theorem 1.3. *Suppose that G and H are Abelian groups, G is finite, $r \in \mathbb{N}$ is a parameter, and $f : G \rightarrow H$ is an injection. Then*

$$\mathbb{P}(f(x+y) = f(x) + f(y)) = O\left(\frac{1}{|G|} \min\{|r \cdot G| |K_{H,r}|, |r \cdot H| |K_{G,r}|\}\right)^\alpha$$

for any $\alpha \leq \max\left\{\frac{1}{5r+1}, \frac{1}{18\lceil \log_2 r \rceil + 7}\right\}$.

Although the statement may appear rather gruesome, Proposition 1.1 follows immediately on taking $r = 2$ since $2 \cdot (\mathbb{Z}/2\mathbb{Z})^n = \{0_{(\mathbb{Z}/2\mathbb{Z})^n}\}$ and $K_{\mathbb{Z}/p\mathbb{Z},2} = \{0_{\mathbb{Z}/p\mathbb{Z}}\}$ for p odd.

Proof of Proposition 1.2. Suppose that $d_1 \mid \cdots \mid d_n$ are the invariant factors of G . Let $r \mid d_1$ be a prime. Since G and H have co-prime order we see that $K_{H,r}$ is trivial and $|r \cdot G| = \frac{d_1}{r} \cdots \frac{d_n}{r}$. Applying Theorem 1.3 we see that

$$\mathbb{P}(f(x+y) = f(x) + f(y)) = O\left(2^{-c(r)n}\right) \text{ where } c(r) = \max\left\{\frac{\log_2 r}{5r+1}, \frac{\log_2 r}{18\lceil \log_2 r \rceil + 7}\right\}.$$

If $p \geq 2^7$ then

$$c(p) \geq \frac{\log_2 p}{18 \log_2 p + 7} = \frac{1}{18 + \frac{7}{\log_2 p}} \geq \frac{1}{19} > \frac{\log_2 17}{79} = c(17).$$

It follows that $c(r) \geq \min\{c(p) : p \leq 2^7 \text{ is prime}\}$. A short calculation shows that this minimum is $c(17)$ and the result is proved. \square

Theorem 1.3 can be applied (again with $r = 2$) to show that $\mathbb{P}(f(x+y) = f(x) + f(y)) = O(p^{-\frac{1}{11}})$ for injections $f : \mathbb{Z}/p\mathbb{Z} \rightarrow (\mathbb{Z}/2\mathbb{Z})^n$ (an example where Proposition 1.2 gives nothing); and $\mathbb{P}(f(x+y) = f(x) + f(y)) = O\left(2^{-\frac{n}{11}}\right)$ for injections $f : (\mathbb{Z}/2\mathbb{Z})^{2n} \rightarrow (\mathbb{Z}/4\mathbb{Z})^n$ (an example where Proposition 1.2 does not apply).

The centred unwrapping map from $f : \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}$ taking $x + p\mathbb{Z}$ to x whenever $x \in \left(-\frac{p}{2}, \frac{p}{2}\right]$ is injective and (supposing that $p = 2k + 1$ is odd) has

$$\begin{aligned} \mathbb{P}(f(x+y) = f(x) + f(y)) &\geq \frac{1}{p^2} \sum_{-\frac{p}{2} < x, y \leq \frac{p}{2}} 1_{\left(-\frac{p}{2}, \frac{p}{2}\right]}(x+y) \\ &= \frac{1}{p^2} \sum_{x=-k}^k \sum_{y=\max\{-k, -k-x\}}^{\min\{k, k-x\}} 1 = \frac{3k^2 + 3k + 1}{4k^2 + 4k + 1} > \frac{3}{4}. \end{aligned}$$

If $q > p$ is another prime then this can be composed with the natural projection $\mathbb{Z} \rightarrow \mathbb{Z}/q\mathbb{Z}$ to give an injection $f : \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}/q\mathbb{Z}$ such that $\mathbb{P}(f(x + y) = f(x) + f(y)) > \frac{3}{4}$.

As a final remark we mention ‘approximate homomorphisms’ between possibly non-Abelian groups have been studied by Moore and Russell. As an example it follows from [MR15, Theorem 3] and a classical result of Frobenius³ that $\mathbb{P}(f(xy) = f(x) + f(y)) = O(|\mathrm{PSL}_2(q)|^{-\frac{1}{6}})$ for injections $f : \mathrm{PSL}_2(q) \rightarrow H$ where $q \geq 5$ and H is Abelian.

In our arguments we regard our groups as endowed with counting measure, so that if G is an Abelian group we define

$$f * g(x) := \sum_y f(y)g(x - y) \text{ for all } x \in G \text{ and } f, g \in \ell_1(G);$$

and similarly

$$\langle f, g \rangle_{\ell_2(G)} := \sum_y f(y)\overline{g(y)} \text{ for all } f, g \in \ell_2(G).$$

In particular, if G and H are Abelian groups with G finite, $f : G \rightarrow H$ is a function, and $\Gamma := \{(x, f(x)) : x \in G\}$ is the graph of f , then $|\Gamma| = |G|$ and

$$(1.1) \quad \frac{1}{|\Gamma|^2} \langle 1_\Gamma * 1_\Gamma, 1_\Gamma \rangle_{\ell_2(G \times H)} = \frac{1}{|G|^2} |\{a, b \in G : f(a + b) = f(a) + f(b)\}| \\ = \mathbb{P}(f(x + y) = f(x) + f(y)).$$

We now turn to the proof of Theorem 1.3 which is primarily done through Proposition 1.4. The overall structure of the argument is a common one in additive combinatorics. We start with the closed graph theorem for groups: that is, the observation that a function between groups is a homomorphism if and only if its graph is a subgroup of the direct product.

The probability that we are interested in (1.1) measures how close the graph of the function is to being a group. There is a well-developed theory, starting with work of Balog and Szemerédi (see [TV06, §2.5]), describing what such sets must look like and it turns out that in Abelian groups of bounded exponent they must be close to genuine subgroups. This is not quite the situation we are in, but arguments of this type can be used to show that if the probability in (1.1) is large then the function must agree with a genuine homomorphism on a large set. This leads to a contradiction.

For our arguments we do not need much of this general theory as a counting argument lets us arrive at a contradiction directly. This is essentially the content of Claim 1 below.

Proposition 1.4. *Suppose that G and H are Abelian groups; G is finite; $\Gamma \subset G \times H$ is such that the coordinate projections restricted to Γ are injective; and $r \in \mathbb{N}$ is a parameter. Then*

$$(1.2) \quad \frac{1}{|\Gamma|^2} \langle 1_\Gamma * 1_\Gamma, 1_\Gamma \rangle_{\ell_2(G \times H)} = O\left(\frac{|r \cdot G| |K_{H,r}|}{|\Gamma|}\right)^\alpha$$

³Specifically [DSV03, Theorem 3.5.1] that for $q \geq 5$, $\mathrm{PSL}_2(q)$ has no non-trivial representation of dimension below $\frac{1}{2}(q - 1)$.

for any $\alpha \leq \max \left\{ \frac{1}{5r+1}, \frac{1}{18\lceil \log_2 r \rceil + 7} \right\}$.

Proof. Write π_G and π_H for the coordinate projections on $G \times H$.

Claim 1. *Suppose that $X, B \subset \Gamma$. Then*

$$\frac{|X + r \cdot B|}{|X|} \geq \frac{|B|}{|K_{H,r}| |r \cdot G|}.$$

Proof. Write $\mathcal{Q} := \{(x, y, z, w) \in X \times (r \cdot B) \times X \times (r \cdot B) : x + y = z + w\}$, and consider the map

$$\psi : \mathcal{Q} \rightarrow X \times (r \cdot B) \times (r \cdot G); (x, y, z, w) \mapsto (x, y, \pi_G(z) - \pi_G(x)).$$

This is well-defined: if $(x, y, z, w) \in \mathcal{Q}$ then $x + y = z + w$, and π_G is a homomorphism so

$$\pi_G(z) - \pi_G(x) = \pi_G(y) - \pi_G(w) \in \pi_G(r \cdot B) - \pi_G(r \cdot B) \subset r \cdot G.$$

Moreover, ψ is an injection: suppose that $\psi(x, y, z, w) = \psi(x', y', z', w')$. Then $x = x'$, $y = y'$, and $\pi_G(z) - \pi_G(x) = \pi_G(z') - \pi_G(x')$. It follows that $\pi_G(z) = \pi_G(z')$ and hence $z = z'$ since π_G restricted to Γ is injective. But then $w' = x' + y' - z' = x + y - z = w$ and the injectivity of ψ follows.

We conclude

$$(1.3) \quad \|1_X * 1_{r \cdot B}\|_{\ell_2(G \times H)}^2 = |\mathcal{Q}| \leq |X| |r \cdot B| |r \cdot G|.$$

On the other hand, if $|X + r \cdot B| \leq L|X|$ then by the Cauchy-Schwarz inequality we have

$$\|1_X * 1_{r \cdot B}\|_{\ell_2(G \times H)}^2 \geq \frac{\|1_X * 1_{r \cdot B}\|_{\ell_1(G \times H)}^2}{|X + r \cdot B|} = \frac{|X|^2 |r \cdot B|^2}{|X + r \cdot B|} \geq \frac{1}{L} |X| |r \cdot B|^2.$$

Combining with (1.3) and cancelling we see that

$$|r \cdot G| \geq \frac{1}{L} |r \cdot B| \geq \frac{1}{L} |\pi_H(r \cdot B)| = \frac{1}{L} |r \cdot \pi_H(B)| \geq \frac{1}{L} \frac{|\pi_H(B)|}{|K_{H,r}|} = \frac{1}{L} \frac{|B|}{|K_{H,r}|},$$

since π_H restricted to Γ is an injection. The claim follows. \square

Write ϵ for the left hand side of (1.2).

Claim 2. *(1.2) holds with $\alpha \leq \frac{1}{5r+1}$.*

Proof. Define a bipartite graph \mathcal{G} with vertex sets two copies of Γ , and $(x, y) \in E(\mathcal{G})$ if and only if $x + y \in \Gamma$. Then $|E(\mathcal{G})| = \epsilon |\Gamma|^2$, and $\Gamma +_{\mathcal{G}} \Gamma := \{x + y : (x, y) \in E(\mathcal{G})\} \subset \Gamma$, so $|\Gamma +_{\mathcal{G}} \Gamma| \leq |\Gamma|$. The Balog-Szemerédi-Gowers Lemma [TV06, Theorem 2.29] can then be applied to give sets $A, B \subset \Gamma$ such that

$$|A|, |B| = \Omega(\epsilon |\Gamma|) \text{ and } |A + B| = O(\epsilon^{-4} |\Gamma|) = O(\epsilon^{-5} |A|).$$

Apply Plünnecke's inequality [TV06, Corollary 6.26] to get a non-empty $X \subset A$ such that (recalling the notation $rB := B + \dots + B$) $|X + rB| = O(\epsilon^{-5r} |X|)$. But then $r \cdot B \subset rB$ and so $|X + r \cdot B| \leq |X + rB| = O(\epsilon^{-5r} |X|)$ and we get the claimed bound from Claim 1 and the fact that $|B| = \Omega(\epsilon |\Gamma|)$. \square

Claim 3. (1.2) holds with $\alpha \leq \frac{1}{18\lceil \log_2 r \rceil + 7}$.

Proof. Apply Lemma 2.2 to get a set $B \subset \Gamma$ such that $x_0 - B = B$ for some $x_0 \in G$ and

$$|B| = \Omega(\epsilon|\Gamma|) \text{ and } |B - B| = O(\epsilon^{-5}|\Gamma|) = O(\epsilon^{-6}|B|).$$

Apply Plünnecke's inequality [TV06, Corollary 6.26] to get a non-empty $Y \subset B$ such that $|Y - 3B| = O(\epsilon^{-18}|Y|)$. Since $2 \cdot B - 2x_0 \subset 2(B - x_0) = -2B$ we get $|Y - B + 2 \cdot B| \leq O(\epsilon^{-18}|Y|)$. By Lemma 2.1 (and the fact that $|B + B| = |B + x_0 - B| = |B - B|$)

$$|B + r \cdot B| = O(\epsilon^{-15})^{\lceil \log_2 r \rceil} |B + B| = O(\epsilon^{-18})^{\lceil \log_2 r \rceil} O(\epsilon^{-6}|B|).$$

We get the claimed bound from Claim 1 with $X = B$, and the fact that $|B| = \Omega(\epsilon|\Gamma|)$. \square

Proof of Theorem 1.3. We can apply Proposition 1.4 to the graph of f i.e. $\Gamma = \{(x, f(x)) : x \in G\}$ in $G \times H$. (π_G is injective on Γ since f is a function, and π_H is injective on Γ since f is injective.). The calculation in (1.1) then gives the bound in the first term in the minimum in Theorem 1.3. A similar argument, applying Proposition 1.4 with $\Gamma = \{(f(x), x) : x \in G\}$ and G and H swapped gives the bound in the second term in the minimum Theorem 1.3. \square

2. SUMSET ESTIMATES

We have taken some care with powers in this note which means that we have needed bespoke versions of Bukh's Theorem [Buk08, Theorem 3] and the Balog-Szemerédi-Gowers Lemma [TV06, Theorem 2.29]. These are proved below through minor variations on the arguments referenced.

The first lemma is proved in roughly the same way as [Buk08, Theorem 15], though we have to take care because our group may have torsion. We do this by appealing to the beautiful [Pet12, Proposition 2.1] of Petridis, the central component in his (2nd) proof of Plünnecke's inequality.

Lemma 2.1. *Suppose that G is an Abelian group; $Y \subset A \subset G$ is finite with $|Y - A + 2 \cdot A| \leq K|Y|$; and $r \in \mathbb{N}$ is a parameter. Then*

$$|X + r \cdot A| \leq K^{\lceil \log_2 r \rceil} |X + A| \text{ for all finite } X \subset G.$$

Proof. Let $\emptyset \neq Z \subset Y$ be such that $\frac{|Z - A + 2 \cdot A|}{|Z|}$ is minimal. By Petridis' lemma [Pet12, Proposition 2.1] we see that

$$(2.1) \quad |Z - A + 2 \cdot A + C| \leq \frac{|Z - A + 2 \cdot A|}{|Z|} |Z + C| \leq K|Z + C| \text{ for all finite } C \subset G.$$

Suppose $k \in \mathbb{N}$. We may assume that G is finitely generated (e.g. by $A \cup X$), so $K_{G,2^{k-1}}$ is finite. Then by (2.1) we have

$$(2.2) \quad |2^{k-1} \cdot (Z - A + 2 \cdot A)| = \frac{|Z - A + 2 \cdot A + K_{G,2^{k-1}}|}{|K_{G,2^{k-1}}|} \leq \frac{K|Z + K_{G,2^{k-1}}|}{|K_{G,2^{k-1}}|} = K|2^{k-1} \cdot Z|.$$

Now, apply the Ruzsa triangle inequality [TV06, Lemma 2.6] to see that

$$\begin{aligned} \left| X + \sum_{i=0}^k 2^i \cdot A \right| &\leq \frac{\left| \left(X + \sum_{i=0}^{k-2} 2^i \cdot A \right) + 2^{k-1} \cdot Z \right| \cdot \left| -2^{k-1} \cdot Z - (-2^{k-1} \cdot A - 2^k \cdot A) \right|}{\left| -2^{k-1} \cdot Z \right|} \\ &\leq \left| X + \sum_{i=0}^{k-1} 2^i \cdot A \right| \cdot \frac{\left| 2^{k-1} \cdot (Z - A + 2 \cdot A) \right|}{\left| 2^{k-1} \cdot Z \right|} \leq K \left| X + \sum_{i=0}^{k-1} 2^i \cdot A \right|, \end{aligned}$$

by (2.2) and the fact that $Z \subset Y \subset A$. It follows by induction that $\left| X + \sum_{i=0}^k 2^i \cdot A \right| \leq K^k |X + A|$ for all $k \in \mathbb{N}_0$.

Let $k := \lceil \log_2 r \rceil$ and write r in binary *i.e.* let $\epsilon_0, \dots, \epsilon_k \in \{0, 1\}$ be such that $r = \epsilon_0 + \epsilon_1 2 + \dots + \epsilon_k 2^k$. Then

$$\left| X + r \cdot A \right| \leq \left| X + \sum_{i=0}^k \epsilon_i 2^i \cdot A \right| \leq \left| X + \sum_{i=0}^k 2^i \cdot A \right| \leq K^k |X + A|$$

as claimed. \square

The second lemma varies the vanilla Balog-Szemerédi-Gowers Lemma by adding some x_0 with $x_0 - T = T$. This means that for sumset purposes we can treat T as symmetric and will not need to bear the cost of applying Pünnecke's inequality to pass between bounds on $|T - T|$ and $|T + T|$.

Lemma 2.2. *Suppose that G is an Abelian group and $S \subset G$ has $\langle 1_S * 1_S, 1_S \rangle_{\ell_2(G)} \geq \epsilon |S|^2$. Then there is a set $T \subset S$ and some $x_0 \in G$ such that*

$$x_0 - T = T, |T| = \Omega(\epsilon |S|) \text{ and } |T - T| = O(\epsilon^{-5} |S|).$$

Proof. For $y, z \in G$ define

$$p(y, z) := \frac{1}{|S|} |(y + S) \cap S \cap (S + z)| 1_S(y) 1_S(z) \leq \frac{1}{|S|} 1_S * 1_{-S}(y - z).$$

Let $x \in S$ be chosen uniformly at random and put $U := S \cap (x - S)$ so that $\mathbb{P}((y, z) \in U^2) = p(y, z)$. Let $c := \frac{1}{18}$ (for reasons that will become clear) and note, by the Cauchy-Schwarz inequality, that

$$\mathbb{E} \left(|U|^2 - \frac{1}{2} c^{-1} |\{(y, z) \in U^2 : p(y, z) \leq c\epsilon^2\}| \right) \geq \mathbb{E} |U|^2 - \frac{1}{2} \epsilon^2 |S|^2 \geq \frac{1}{2} \epsilon^2 |S|^2.$$

It follows that we can pick $x \in S$ such that

$$|U| \geq \frac{\epsilon}{\sqrt{2}} |S| \text{ and } |\{(y, z) \in U^2 : p(y, z) > c\epsilon^2\}| \geq (1 - 2c) |U|^2.$$

By averaging, the set $R := \{y \in U : |\{z \in U : p(y, z) > c\epsilon^2\}| \geq (1 - 6c) |U|\}$ has $|R| \geq \frac{2}{3} |U|$. Since $x - U = U$ we see that $x - R \subset U$ and hence $T := R \cap (x - R)$ has $|T| \geq \frac{1}{3} |U|$ (by the pigeon-hole principle) and $T = x - T$.

For each $s \in T - T$ there are elements $y, w \in T$ such that $s = y - w$. Since $y, w \in R$ and $1 - 6c \geq \frac{2}{3}$, the pigeon-hole principle tells us that there are at least $\frac{1}{3}|U|$ elements $z \in U$ such that $p(y, z) > c\epsilon^2$ and $p(w, z) > c\epsilon^2$. Hence

$$\begin{aligned} \frac{|U|}{3} \cdot (c\epsilon^2)^2 |S|^2 &< |S|^2 \sum_{z \in U} p(y, z)p(w, z) \\ &\leq \sum_{z \in U} 1_S * 1_{-S}(y - z) 1_{-S} * 1_S(z - w) \leq 1_S * 1_{-S} * 1_{-S} * 1_S(y - w). \end{aligned}$$

It follows that

$$|T - T| \cdot \frac{|U|}{3} \cdot (c\epsilon^2)^2 |S|^2 \leq \sum_{s \in G} 1_S * 1_{-S} * 1_S * 1_{-S}(s) = |S|^4,$$

and the lemma is proved with $x_0 = x$. □

ACKNOWLEDGEMENT

The author thanks Terry Tao for bringing the problem to his attention, and an anonymous referee for their improvements.

REFERENCES

- [Buk08] B. Bukh. Sums of dilates. *Combin. Probab. Comput.*, 17(5):627–639, 2008.
- [DSV03] G. Davidoff, P. Sarnak, and A. Valette. *Elementary number theory, group theory, and Ramanujan graphs*, volume 55 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 2003.
- [Lov] S. Lovett. <http://mathoverflow.net/questions/208384/approximate-homomorphisms>.
- [MR15] C. Moore and A. Russell. Approximate representations, approximate homomorphisms, and low-dimensional embeddings of groups. *SIAM J. Discrete Math.*, 29(1):182–197, 2015.
- [Pet12] G. Petridis. New proofs of Plünnecke-type estimates for product sets in groups. *Combinatorica*, 32(6):721–733, 2012.
- [TV06] T. C. Tao and H. V. Vu. *Additive combinatorics*, volume 105 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2006.

MATHEMATICAL INSTITUTE, UNIVERSITY OF OXFORD, RADCLIFFE OBSERVATORY QUARTER, WOODSTOCK ROAD, OXFORD OX2 6GG, UNITED KINGDOM
E-mail address: tom.sanders@maths.ox.ac.uk