technische universität
dortmund

GENERIC SUBGROUPS OF GROUP AMALGAMS

Benjamin Fine, Alexei Myasnikov,
Gerhard Rosenberger

Fakultät für Mathematik
Technische Universität Dortmund
Vogelpothsweg 87
44227 Dortmund

Preprint Nr. 2008-05
April 2008

tu-dortmund.de/MathPreprints

GENERIC SUBGROUPS OF GROUP AMALGAMS

Benjamin Fine, Alexei Myasnikov, Gerhard Rosenberger

Abstract. For many groups the structure of finitely generated subgroups is generically simple. That is with asymptotic density equal to one a *randomly chosen* finitely generated subgroup has a particular well-known and easily analyzed structure. For example a result of D.B.A.Epstein says that a finitely generated subgroup of $GL(n, \mathbb{R})$ is generically a free group. We say that a group G has the **generic free group property** if any finitely generated subgroup is generically a free group. Further G has the **strong generic free group property** if given randomly chosen elements $g_1, ..., g_n$ in G then generically they are a free basis for the free subgroup they generate. In this paper we show that for any arbitrary free product of finitely generated infinite groups satisfies the strong generic free group property. There are also extensions to more general amalgams - free products with amalgamation and HNN groups. These results have implications in cryptography. In particular several cryptosystems use random choices of subgroups as hard cryptographic problems. In groups with the generic free group property any such cryptosystem may be attackable by a length based attack.

1. Introduction

If $\mathcal{P}$ is a group property and G is a group then we say that subgroups of G are *generically* $\mathcal{P}$ if a randomly chosen subgroup H of G generically has property $\mathcal{P}$. Equivalently this means that the asymptotic density (see section 2) of subgroups H of G that have property $\mathcal{P}$ is one. For example a result of D.B.A.Epstein [E] says that a finitely generated subgroup of $GL(n, \mathbb{R})$ is generically a free group. In particular this can be applied to the classical Modular group $PSL(2, \mathbb{Z})$ so that with asymptotic density one, n randomly chosen 2×2 projective integral matrices of determinant one generate a free group. Recall that group theoretically the Modular group $PSL(2, \mathbb{Z})$ is a nontrivial free prduct $\mathbb{Z}_2 \star \mathbb{Z}_3$. Although this result and Epstein's proof seem specialized to linear groups (see section 3), this type of behavior turns out to be not uncommon. For many groups the structure of finitely generated subgroups is generically simple. That is with asymptotic density one a *randomly chosen* finitely generated subgroup has a particular well-known and easily analyzed structure.

In general we say that a group G has the **generic free group property** if a finitely generated subgroup is generically a free group. In this language Epstein's result is that the group $GL(n, \mathbb{R})$ satisfies the generic free group property. Further G has the **strong generic free group property** if given randomly chosen elements $g_1, ..., g_n$ in G then generically they are a free basis for the free subgroup they generate. Even stronger we say that G satisfies the **dominant Nielsen property** if given randomly chosen elements $g_1, ..., g_n$ in G then generically they are a minimal Nielsen basis for the free subgroup they generate. Jitsukawa [J] showed that finitely generated free groups have the strong generic free group property while Myasnikov and Ushakov [MSU] showed that pure braid groups also have the

strong generic free group property. This last result has applications in the cryptanalysis of both the Ko-Lee cryptosystem and the Anshel-Anshel-Goldfeld cryptosystem (see [SU] and [MU]). Finally Gilman, Myasnikov and Osin [GMO] showed that torsion-free hyperbolic groups have the generic free group property.

In this paper we prove that an arbitrary free product of finitely generated infinite groups satisfies the strong generic free group property. Under some restrictions more general arbitrary amalgams also satisfy the strong generic free group property. These results have implications in nonabelian group cryptography (see [SU],[MU]). In cryptographic methods using nonabelian groups encryption is usually done within subgroups of given finitely presented groups. As one way functions for cryptography, "hard" group theoretical problems such as the conjugator search problem are used (see [AAG]). In these protocols random choices of subgroups are made. In many cases, even though the overall group theoretical problem is hard to solve, generically the subgroups have a nice structure in which the problem can be solved. This affects the security of the cryptosystem and must be dealt with in both implementing the cryptosystem and in devising parameters for the implementation (see [BMS]). Cryptosystems involving these methods employing groups that have either the generic free group property or the strong generic free group property are subject to length based attacks similar to attacts on pure free group cryptosystems (see [SU] and [MiU]).

The proofs of our main results depend upon the fact that in a free product a random choice of finitely many elements of bounded syllable length has asymptotic density zero. This is related to a result of Goldstein [G] that says that in a free group elements of bounded length have asymptotic density zero.

The outline of this paper is as follows. In section 2 we explain the concept of asymptotic density and the meaning of choosing random elements and random finitely generated subgroups of amalgams. In section 3 we prove our main result for free products. We also present an alternative proof of the weaker result that an arbitrary free product of infinite groups has the generic free group property. Although this weaker result is subsumed by the main result this alternative proof gives insight into what is happening generically relative to Kurosh bases. In section 4 we consider some extensions of the results to more general amalgams. Along these lines we show that many cyclically pinched one-relator groups and in particular all orientable surface groups of genus 2 or greater satisfy the strong generic free group property.

2. Asymptotic Density and Random Elements

Our two main results concerning arbitrary free products are the following - the first of which says that an arbitrary free product of inifnite groups satisfies the generic free group property and the second which says that an arbitrary free product of infinite groups satisfies the strong generic free group property.

Theorem 3.1. *Let A and B be arbitrary finitely generated infinite groups and let $G = A \star B$ be their free product. Then a finitely generated subgroup of G is generically free.*

Theorem 3.2. *Let A and B be arbitrary finitely generated infinite groups and let $G = A \star B$ be their free product. Let $x_1, ..., x_n$ be n randomly chosen elements from G. Then generically these elements form a free basis for the subgroup they generate.*

Before proving these we explain the concept of asymptotic density and generic subgroups and then describe how we choose random elements and random finitely generated subgroups

in free products. These methods carry through to more general amalgams.

Asymptotic density is a general method to compute densities and/or probabilities on infinite discrete sets where each individual outcome is tacitly assumed to be equally likely. The origin of aymptotic density lie in the attempt to compute probabilities on the whole set of integers where each integer is considered equally likely. The method can also be used where some probability distribution is assumed on the elements. It has been effectively applied to determining densities within infinite discrete finitely generated groups where random elements are considered as being generated from random walks on the Cayley graph of the group. The paper by Borovik, Myasnikov and Shpilrain [BMS] provides a good general description of this method in group theory. Let $\mathcal{P}$ be a group property and let G be a finitely generated group. We want to determine the measure of the set of elements which satisfy $\mathcal{P}$. For each positive integer n let B_n denote the n-ball in G. Let $|B_n|$ denote the actual size of B_n (which is an integer since G is finitely generated) or the measure of $|B_n|$ if a distribution has been placed on the elements of G. Let S be the set of elements in G satisfying $\mathcal{P}$. The asymptotic density of S is then

$$\lim_{n\to\infty} \frac{|S \cap B_n|}{|B_n|}$$

provided this limit exists. We say that the property $\mathcal{P}$ is **generic** if the asymptotic density of the set S of elements satisfying $\mathcal{P}$ is one.

This concept can be easily extended to properties of finitely generated subgroups, We consider the asymptotic density of finite sets of elements that generate subgroups that have a considered property. For example to say that a group has the generic free group property we mean that

$$\lim_{m,n\to\infty} \frac{|S_m \cap B_n|}{|B_n|} = 1$$

where S_m is the collection of finite sets of elements of size m that generate a free subgroup.

Clearly these definitions depend on how we choose random elements in G. We now describe how to choose random elements and random finitely generated subgroups in a free product. Let $G = A \star B$ where A and B are infinite groups. Since we will be dealing with finitely generated subgroups without loss of generality we may assume that the factors A and B are finitely generated.

Now assume that $A =< a_1, ..., a_N >$ and $B =< b_1, .., b_M >$ but we make no assumption on the distributions within A and B. Essentially choosing a random element in $A \star B$ is a random walk on the Bass-Serre tree with a random choice from each vertex. To randomly choose an element we do the following. Choose a 0 or a 1 to see whether an element starts with an A element or a B element. We then randomly choose a integer n to be the syllable length. To pick an element first choose 0 or 1. Suppose the choice is 0. Then A is picked first. We then randomly pick an A element followed by a random B element and so on. The probability of choosing A elements and B elements depends on the distribution of elements within the factors. Syllable length is random on the natural numbers even if we don't know the distribution in the factors.

To permit counting we are going to randomly choose within the total random choice in finite balls in A and B. (These choices will depend on the distribution in the factors but will not affect our final densities.)

To choose a random element we make 4 random choices:

(1) n = syllable length
(2) m = total length in the alphabet on the generators
(3) A n-partition $k_1, ..., k_n$ of m with no $k_i = 0$
(4) Choose 0 or 1

To then pick a random element we do the following:

The 0 or 1 pick says that you're starting with either A or B. Suppose its 0 so we pick first from A. We choose a random k_1 length element in A. Notice that this depends on the distribution in A but that doesn't affect our final result. We then pick a random k_2 length element in B and so on.

Notice the probabilities of picking elements in A and B of shorter lengths may not be the same as longer lengths or vice versa but all we are interested in is the relative picking of fixed syllable length versus arbitrary syllable length.

Randomly choosing a finitely generated subgroup is equivalent to randomly choosing an integer p and then randomly choosing p elements.

3. Generic Subgroups of Free Products

In this section we prove the two main results for free proucts; Theorem 2.1 and the stronger Theorem 2.2. Before looking at these results we look at Epstein's result in $GL(n, \mathbb{R})$ to gain some insight into what is occurring there. $GL(n, \mathbb{R})$ lives in R^{n^2} that is n^2-dimensional space. Consider standard measure on this space and let $E_n(\mathbb{R})$ be the set of all real $n \times n$ matrices. Since

$$det : E_n(\mathbb{R}) \to \mathbb{R}$$

is a continuous function it follows that the set of singular matrices has measure zero and therefore $GL(n, \mathbb{R})$ is generically n^2-dimensional. Suppose $M_1, ..., M_k$ are k randomly chosen matrices in $GL(n, \mathbb{R})$. If they did not generate a free group then there is a nontrivial relation on $M_1, ..., M_k$ and hence a nontrivial word W with $W(M_1, ..., M_k) = I$. This imposes an algebraic relation on the elements in $M_1, ..., M_k$ and thus implies that as elements of R^{n^2} they live in a nontrivial algebraic variety and hence a lower dimensional space. It follows that in this case, that is $M_1, .., M_K$ do not generate a free group, the group generated by $M_1, ..., M_k$ must have measure zero. Although not exactly the same, our proof will use that elements of bounded syllable length in a free product have asymptotic density 0.

We first look at the stronger result Theorem 2.2.

Theorem 3.2. *Let A and B be arbitrary finitely generated infinite groups and let $G = A \star B$ be their free product. Let $\{x_1, ..., x_n\}$ be n randomly chosen elements from G. Then generically these elements are a free basis for the subgroup they generate.*

We will denote the asymptotic density of types of subsets S of the group G by $\rho(S)$ when this asymptotic density exists. The proof of Theorem 2.2 will follow from a series of lemmas.

Lemma 3.1. *In $G = A \star B$ the asymptotic density of elements of syllable length one is zero*

Proof. Fix generating systems for A and B. For any distribution on A and B the number of elements of minimal length m in the given generating system is less than the number of strings of length m. Further for each syllable we are randomly choosing from A or B. Therefore for this probability and asymptotic density question we may assume that A and B are free on their generating systems and count strings.

It is straighforward that in randomly choosing positive integers the asymptotic density of any bounded set is zero. Consider, for example, randomly choosing the integer 1. In the first n the probability is clearly $\frac{1}{n}$. Letting $n \to \infty$ gives the asymptotic density of 0.

Now let G_{mn} denote the number of strings in $A \star B$ of syllable length n and total length m. Let G_1 be the elements of syllable length 1 that is elements of either A or B. Since in randomly picking elements in G we must make a choice of syllable length the asymptotic density of chooisng an element of syllable length one is less than or equal to randomly choosing the integer 1 among the natural numbers $\mathbb{N}$. Hence it follows that

$$\lim_{n\to\infty} \frac{|G_1 \cap G_{nm}|}{|G_{mn}|} = 0$$

independent of m. Therefore the asymptotic density is zero.

Notice that if S is a finite subset of G then the asymptotic density that S contains an element of syllable length one is less than or equal to the overall aymptotic density of radnomly choosing an element of syllable length one. Therefore we have the following corollary.

Corollary 3.1. *If S is a finite set in $A \star B$ then the asymptotic density of S is zero if S has any elements of syllable length one.*

Further if k is a fixed positive integer then the same argument shows that choosing a random element of syllable length bounded by k is also zero.

Corollary 3.2. *If k is a fixed positive integer then asymptotic density of randomly choosing an element of $A \star B$ of syllable length bounded by k is zero.*

Lemma 3.2. *Let $S = \{x_1, ..., x_n\}$ be a finite set of elements. Then*

$$\rho(\{x_1, .., x_n\} \text{ is a free basis }) = \rho(\{x_1, .., x_n\} \text{ is a free basis}$$

$$\text{given that } x_1, ..., x_n \text{ all have syllable length } > 1)$$

Here by a free basis we mean a free basis for the subgroup they generate.

In essence this lemma says that we may assume that in choosing a finitely generated subgroup each generator has syllable length > 1.

Proof. Let
U be the set of those $\{x_1, ..., x_n\}$ such that $\{x_1, ..., x_n\}$ is a free basis. Let
V be the subset of U such that all $x_1, .., x_n$ have syllable length ¿ 1*and*
$W = V'$ the subset of U such that at least one of $x_1, ..., x_n$ has syllable length 1.
We then have

$$\rho(U) = \rho(U/V)\rho(V) + \rho(U/V')\rho(V')$$

but

$$\rho(V') = \rho(\text{ at least one of } x_1, ..., x_n \text{ has syllable length } 1) = 0$$

and

$$\rho(V) = 1$$

Lemma 3.3. *Let A be an infinite finitely generated group. Then the aymptotic density of picking two random elements a, b and having $a = b^{-1}$ is zero.*

Proof. Let $A = F/N$. Then a result of Olshanski [O] shows that the asymptotic density of randomly choosing an element of F which is in N is zero. The lemma is then equivalent to choosing two elements of F, say u, v, with $uv^{-1} \in N$.

Lemma 4. *Let $x_1, ..., x_n \in G = A \star B$ be all of syllable length > 1. Then*

$$\rho(\{x_1, ..., x_n\} \text{ is a free basis }) = 1$$

Here by a free basis we mean a free basis for the subgroup they generate.

Proof. Suppose that we choose $x_1, .., x_n$ each of syllable length > 1. Then $x_1, ..., x_n$ cannot satisfy a nontrivial relation unless the final syllable of one of them cancels the initial syllable of another. Therefore the probability of being a free basis reduces to the probability of randomly choosing two elements g_1, g_2 from either A or B and having $g_1^{-1} = g_2$. It follows from Lemma 3.3 that the asymptotic density in doing this is zero. Hence the random elements, with asymptotic density one, must generate a free group.

Proof. (Theorem 2.2) We can string these lemmas together to prove Theorem 2.2. Suppose that $\{x_1, ..., x_n\}$ is a randomly chosen finite subset from $G = A \star B$. From Lemma 2 the asympotitic density that they form a free basis is the same as the asymptotic density that they form a free basis given that all the elements have syllable length ¿ 1. Therefore generically we may assume that each x_i has syllable length greater than 1. Then from lemma 4 the asymptotic density that they form a free basis is 1 completing the proof.

We now give an alternative proof of the weaker result that an arbitrary free product of infinite groups has the generic free group property.

Theorem 2.1. *Let A and B be arbitrary finitely generated infinite groups and let $G = A \star B$ be their free product. Then G satisfies the generic free group property.*

Proof. Let $H =< g_1, ..., g_n >$ be a randomly chosen finitely generated subgroup of $A \star B$. From the Kurosh theorem H must have the following structure

$$H = F \star A_1 \star ... \star A_l \star B_1 \star ... \star B_k$$

where F is a free group and A_i is a conjugate of a subgroup of A and B_j is a conjugate of a subgroup of B. An easy modification of Lemma 3.1 above shows that randomly choosing a conjugate of a subgroup of A or B must have asymptotic density zero. Therefore generically H is F, the free group part.

We could also further formalize this by randomly choosing Kurosh bases, that is modifying the randomization procedure by only choosing Kurosh bases and counting strings within these. The crux of this counting also comes down to the fact that choosing syllable length is generically zero.

4. Generic Subgroups of More General Amalgams

In this section we consider extensions of the string generic free group property to more general group amalgams. In extending these results we must be careful about very general

statements. A great deal of nonstandard behavior can be exhibited by amalgams. For example the two-generator Fuchsian group

$$< a, b; a^2b^2 = 1 >=< a; > \underset{\{a^2=b^{-2}\}}{\star} < b; >$$

is solvable and hence cannot satisfy the strong generic free group property.

Similarly the infinite dihedral group $\mathbb{Z}_2 \star \mathbb{Z}_2$ is also solvable and hence cannot satisfy the strong generic free group property.

To handle more general amalgams the following straightforward result is extremely useful.

Theorem 4.1. *Let G be a group and N a normal subgroup. If the quotient G/N satisfies the strong generic free group property then G also satisfies the strong generic free group property.*

Proof. If any quotient G/N satisfies the strong generic free group property it is clear that G must be infinite. Let $g_1, ..., g_n$ be finitely many randomly chosen elements of G. Since G is infinite then an easy modification of Olshanskii's result used in the proof of Lemma 3.3 shows that generically $g_1, ..., g_n$ are not in N.

It follows that their images $\overline{g}_1, ..., \overline{g}_n$ in G/N are nontrivial. Since G/N satisfies the strong generic free group property then generically in G/N the elements $\overline{g}_1, ..., \overline{g}_n$ are a free basis for the subgroup they generate. Since the rank is the same their preimages $g_1, .., g_n$ are also a free basis for the subgroup of G they generate. Since $g_1, ..., g_n$ are arbitrary and generically do not fall in N it follows that G satisfies the strong generic free group property.

Using this we can now prove.

Theorem 4.2. *Let A and B be arbitrary finitely generated infinite groups and let $G = A \underset{H}{\star} B$ be their amalgamated free product. Let H_1 and H_2 be the copy of H in A and B respectively. Suppose that $A/N(H_1)$ is infinite and $B/N(H_2)$ is infinite where $N(H_i)$ is the normal closure of H_i in the respective factors. Then G satisfies the strong generic subgroup property.*

Proof. Let H_1 be the copy of H in A and H_2 the copy of H in B so that the group G has the presentation

$$G =< A, B; rel(A), rel(B), H_1 = H_2 > .$$

Consider in G the normal closure $N(H)$ of the subgroup H. Then the quotient has the presentation

$$G/N(H) =< A, B; rel(A), rel(B), H_1 = H_2 = \{1\} > .$$

This is easily seen to be the free product of $A/N(H_1)$ and $B/N(H_2)$ and therefore

$$G/N(H) \cong A/N(H_1) \star B/N(H_2).$$

Since each factor is infinite it follows from Theorem 3.2 that $G/N(H)$ satisfies the strong generic subgroup property. From Theorem 4.1 then so does G.

Recall that a **cyclically pinched one-relator group** is a group with a finite presentation of the form

$$G = F_1 \underset{\{U=V\}}{\star} F_2$$

where F_1, F_2 are finitely generated free groups and U, V are nontrivial words in the respective free groups. If U is not a power of a primitive element in F_1 and V is not a power of a primitive element in F_2 then the quotient of F_1 and F_2 by the normal closure of U and V respectively is a nontrivial, infinite one-relator group. It follows that Theorem 4.2 can be applied.

Corollary 4.1. *Let G be a cyclically pinched one-relator group as above. Assume that U and V are not a power of a primitive element in F_1 and F_2 respectively. Then G satisfies the strong generic subgroup property.*

In particular any orientable surface group of genus $g \geq 2$ falls into the class of cyclically pinched one-relator groups.

Corollary 4.2. *Any orientable surface group of genus $g \geq 2$ and any nonorientable surface group of genus $g \geq 4$ satisfies the strong generic subgroup property.*

The case with HNN groups becomes even more complicated but some things can be proved as consequences of the amalgam result above. Notice first however that any HNN group with free part of rank ≥ 2 must have a free quotient of rank ≥ 2 and hence satisfy the strong generic subgroup property.

Lemma 4.1. *Any HNN group with free part of rank > 1 satisfies the strong generic subgroup property.*

Therefore only the case where the free part has rank 1 must be considered.

Theorem 4.3. *Let G be an HNN extension of the group B with a presentation*

$$G =< t, B; rel(B), t^{-1}Ut = V >$$

with U, V nontrivial isomorphic subgroups of B. Let $N_B(< U, V >)$ be the normal closure of the subgroup $< U, V >$ in B. Then if $B/N_B(< U, V >)$ is infinite G satisfies the strong generic subgroup property.

Proof. Let $N = N_G(U)$ be the normal closure of the subgroup U in G. Then

$$G/N =< t, B; rel(B), U = \{1\}, V = \{1\} > \cong < t > \star B/N_B(< U, V >).$$

Since each factor is infinite again from Theorem 4.1 it follows that G satisfies the strong generic subgroup property.

Extensions of centralizers play a large role in the study of the elementary theory of free groups. Recall that if B is a group and $U \in B$ then a **rank one extension of centralizers** of B is a group with a presentation

$$G =< t, B; rel(B), t^{-1}UT = U > .$$

Theorem 4.4. *Let G be a rank one extension of centralizers of the group B. Suppose G has a presentation*

$$G =< t, B; rel(B), t^{-1}Ut = U >$$

wihere U is a nontrivial element of B. If $B/N_B(U)$ is infinite, where $N_B(U)$ is the normal closure of U in B, then G satisfies the strong generic subgroup property .

Proof. Let $N = N_G(U)$ the normal closure of U in G. Then

$$G/N =< t, B; rel(B), U = 1 >\cong< t > \star B/N_B(U).$$

As in the previous proof since each factor is infinite it follows that G satisfies the strong generic subgroup property.

We close by briefly mentioning the situation where the factors are finite. We must be careful in this case even for free products. As we mentioned the infinite dihedral group $\mathbb{Z}_2 \star \mathbb{Z}_2$ is solvable so cannot satisfy the strong generic subgroup property. However if at least one factor has order greater than 2, the Kurosh basis analysis yields the weaker generic free group property.

Theorem 4.5. *Let $G = A \star B$ be a nontrivial free product. If at least one factor has order greater than 2 then G satisfies the generic free group property.*

References

[AAG] I.Anshel, M. Anshel and D. Goldfeld, *An Algebraic Method for Public Key Cryptography*, Math.Res. Lett, **6** (1999), 287-291.

[Ar] G.Arzhansvea, *Generic Properties of Finitely Presented Groups and Howson's Theorem*, Comm. Alg, **26** (1998), 3783-3792.

[Ar] G.Arzhansvea and A. Olshanskii, *Genericity of the Class of Groups in Which Subgroups with a Lesser Number of Generators are Free*, Mat. Zametki **59** (1996), 489-496.

[BMS] A.Borovik, A.G. Myasnikov and V.Shpilrain, *Measuring Sets in Infinite Groups*, Cont. , H Math. **298** (2002), 21-42.

[E] D.B.A. Epstein, *Almost all Subgroups of Lie Group are Free*, J. Alg. **19** (1971), 261-262.

[GMO] R.Gilman, A.G. Myasnikov and D.Osin, *Bounded Nielsen Property in Hyperbolic Groups*, to appear.

[G] R.Goldstein, *The Density of Small Words in a Free Group is Zero*, Cont. Math. **360** (2004), 47-50.

[J] T. Jitsukawa, *Malnormal Subgroups of Free Groups*, Cont. Math. **298** (2002), 83-96.

[MU] A.D.Myasnikov and A.Ushakov, *Length Based Attack and Braid Groups:Cryptanalysis of Ahsel-Anshel-Goldfeld Key Exchange Protocol*, Public Key Cryptography - PKc 2007, vol. Lecture Notes in Computer Science, Springer, 2007.

[MSU] A.G. Myasnikov, V.Shpilrain and A. Ushakov, *A Practical Attack on Some Braid Group Based Cryptographic Protocols*, CRYPTO 2005 -Lecture Notes in Computer Science **3621** (2005), 86-96.

[SU] V.Shpilrain and A. Ushakov, *The Conjugacy Search Problem in Public Key Cryptography; Unnnecessary and Insufficient*, Applicable Algebra in Engineering,Communication and computing **17** (2006), 285-289.

Benjamin Fine, Department of Mathematics, Fairfield University, Fairfield, Connecticut 06430, United States

Alexei Myasnikov, Department of Mathematics, McGill UNiversity, Montreal, Canada

Gerhard Rosenberger, Department of Mathematics, TU Dortmund, 44227 Dortmund, Germany